UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

BERNADINE GRIFFITH; et al., individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

TIKTOK, INC., a corporation; BYTEDANCE, INC., a corporation,

Defendants.

Case No. 5:23-cv-00964-SB-E

DECLARATION OF ZUBAIR SHAFIQ, PH. D., IN SUPPORT OF PLAINTIFFS' MOTION FOR CLASS CERTIFICATION

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

I, Zubair Shafiq, declare as follows:

1. Counsel for Plaintiffs retained me to provide expert analysis and, if requested, expert testimony. I have personal knowledge of the matters set forth herein and am competent to testify.

2. I submit this declaration in connection with Plaintiffs' Motion for Class Certification.

3. Attached is a true and correct copy of the Expert Declaration that I prepared in connection with this matter, dated June 21, 2024. The opinions I provided therein are true and correct to the best of my knowledge.

4. The Declaration contains statements of my opinions formed to date and the bases and reasons for those opinions. I understand from counsel that discovery in this case is ongoing, and I may offer additional opinions based on further review of materials in this case. I reserve the right to amend or supplement my opinions based on further discovery and information provided in this case that was not available to me at the time I prepared this Declaration.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed this 21st day of June, 2024, in Davis, California.

Zubair Shafiq, Ph.D.

ATTORNEYS EYES' ONLY

IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

BERNADINE GRIFFITH, et al., individually and on behalf of all others similarly situated, Plaintiffs, v. TIKTOK, INC., a corporation; BYTEDANCE, INC., a corporation, Defendants.	Case No. 5:23-cv-00964-SB-E

DECLARATION OF ZUBAIR SHAFIQ, PH.D. IN SUPPORT OF PLAINTIFFS' MOTION FOR CLASS CERTIFICATION

June 21, 2024

Table of Contents

List of Figures

I. INTRODUCTION

1. My name is Zubair Shafiq, Ph.D. I am an Associate Professor of Computer Science at the University of California-Davis. I have been retained by counsel for Plaintiffs to serve as an independent expert in this litigation and to provide opinions and testimony regarding the technology and practices at issue with respect to the Pixel and Events API products developed and distributed by Defendants TikTok Inc. and ByteDance Inc. (together, "TikTok").

2. This Declaration contains statements of my opinions formed to date and the bases and reasons for those opinions. I understand from counsel that discovery in this case is ongoing, and I may offer additional opinions based on further review of materials in this case, including opinions and/or testimony of other expert witnesses. I reserve the right to amend or supplement my opinions based on further discovery and information provided in this case that was not available to me at the time I prepared this Declaration, as well as based on further information, analysis, or opinions provided by TikTok or experts retained by TikTok.

3. I have had full access to every document produced in this case and to all deposition transcripts, written interrogatory responses, and data produced. I was freely allowed to conduct searches and view any document produced in this litigation for the purpose of preparing this Declaration, and I and a team of consultants working under my supervision spent many hours independently searching for and reviewing documents produced in this case and reviewing the deposition transcripts, written interrogatory responses, and data and information produced.

4. I also reviewed public materials, including TikTok support pages for the TikTok Pixel, TikTok Events API, and related products at issue in this case.

5. The list of documents and materials I have considered and relied upon are cited in line throughout the Declaration.

6. The code and data underlying my testing and analysis are attached as **Appendix B**.

7. The opinions expressed in this Declaration are based on my own personal knowledge, professional judgment, and my analysis of the materials and information I considered in preparing this Declaration, which are listed throughout.

8. I am being compensated for my work in this case at the rate of $750 per hour, which is my standard hourly rate. My compensation is not dependent on and in no way affects the substance of my opinions. Nor does my compensation depend on the outcome of this proceeding. I understand that, should there be any recovery in this case, I will be excluded from any disbursement of funds.

II. SUMMARY AND SCOPE OF OPINION

9. For the purposes of this Declaration, which I understand may not be the final Report that I am asked to provide in this case, I was asked by counsel to perform the following analyses:

- Explain how the TikTok Pixel[1] and TikTok Events API function and investigate the data that they collect when installed on a website or server, respectively.
- Investigate any variability in the data collected by TikTok Pixel across different websites and across different web browsers.
- Investigate any variability in the storage and usage of data collected by TikTok Pixel and TikTok Events API.
- Explain whether and, if so, how the data that TikTok collects on non-TikTok users through the Pixel and Events API could be used to identify Class Members in this case.
- Investigate the type of data collected by Google for its Ipsos Screenwise panel and compare that data to the data collected by TikTok Pixel and/or TikTok Events API.

10. At a high level, and as described in greater detail below, I conclude that TikTok Pixel uniformly and automatically collects certain categories of data from visitors to websites that

[1] I use the term "pixel" (lower case) to refer to pixels generally, and "Pixel" (upper case) to refer specifically to the TikTok Pixel.

use the Pixel. The data collected by TikTok Pixel is agnostic to whether that website visitor is a TikTok user or not. [redacted], TikTok Pixel's data collection is real-time and contemporaneous with the loading of the webpage. The Pixel also consumes measurable storage on the browsers or devices of webpage visitors that visit websites that use the Pixel.

11. Based on my public testing of websites using TikTok Pixel, including riteaid.com, I conclude that TikTok Pixel automatically collects the following seven categories of data for all events, including the default "PageView" event: (a) Timestamp; (b) IP Address; (c) User Agent; (d) Cookies; (e) URL; (f) "Event Information"; and (g) "Content Information."[2] Among these default data categories automatically collected by the Pixel, IP Address, User Agent, and Cookies are identifiers, *i.e.*, data that can identify the website visitor. Event Information and Content Information constitute data on browsing history, *i.e.* data that reveals what a website visitor was doing on a webpage. In particular, my testing shows that TikTok Pixel automatically collects information about the precise sequence of actions performed by a website visitor on a website with the Pixel deployed. Finally, the URL captures both personally identifying information and sensitive content. My analysis of TikTok's sample of data that it collected with Pixel and Events API within an hour on March 28, 2024, reveals that TikTok [redacted]

[2] "Event Information" and "Content Information" are my own terms that describe and categorize certain data that TikTok Pixel automatically collects. The data encompassed within these two categories are further described in Section V.A of this Declaration.

12. I further developed a methodology to test for any variability in TikTok Pixel's data collection across different websites. Based on that methodology and its deployment on 2,000 URLs with TikTok Pixel, I conclude that the Pixel's data collection is uniform across websites and that TikTok Pixel collected Timestamp, IP Address, User Agent, Cookies, URL, and Event Information in 100.0% of the websites. TikTok Pixel collected Content Information on up to 98.0% of the websites. I describe in Section V.D why the 98.0% number does not detract from the conclusion that TikTok Pixel uniformly collected Content Information from non-TikTok users. I reserve the right to amend, modify, and supplement the methodology or to conduct additional testing should new information become available to me during discovery.

13. I also developed a methodology to test any variability in TikTok Pixel's default data collection across different web browsers (*i.e.*, to test whether the Pixel collects data differently from a website like riteaid.com when the website is visited on the Chrome browser versus the Safari browser). I conclude that there is no substantial variability in TikTok Pixel's data collection across four different web browsers (Chrome, Safari, Edge, and Firefox) that together account for more than 95% of the browser market share in the United States. I reserve the right to amend, modify, and supplement the methodology or to conduct additional testing should new information become available to me during discovery.

14. TikTok Events API is another tool developed and marketed by TikTok that collects identifiers and browsing information from a non-TikTok website's server.[3] The Pixel and Events API share commonalities. Just like with TikTok Pixel, the data collected by TikTok Events API is

[3] Unlike the Pixel which is embedded into the source code of the website and thus transmits data from the website visitor's web browser to TikTok's server, Events API is a server-to-server tool that transmits data from the website's server to TikTok's server. This feature means that whether a website server uses Events API is not publicly available information, and data collection by TikTok via the Events API is not testable via public means. TikTok has produced a list of advertisers whose servers use the Events API.

agnostic to whether a website visitor is a TikTok user or not. Just like TikTok Pixel, the data collection by the TikTok Events API is real-time and contemporaneous with the loading of the webpage. Just like TikTok Pixel, TikTok Events API can collect data, including the seven categories discussed above in connection with the Pixel. Unlike the Pixel, however, Events API uses a server-to-server data collection mechanism and thus can circumvent ad blockers and other tracking restrictions on website visitors' web browsers.

15. Based on my review of TikTok's internal documentation and interrogatory responses provided in this litigation thus far, I conclude that TikTok [redacted]

16. Class Members can be identified or verified using the data collected through the TikTok Pixel and Events API itself.

17. Based on publicly available information on the Google Ipsos Screenwise panel, the categories of data collected by Google in that program and those collected by TikTok via the Pixel and Events API are comparable and consist, at a high level, of identifiers and browsing history.

III. QUALIFICATIONS

18. I am an Associate Professor of Computer Science at the University of California-Davis, where I lead a research lab focused on online privacy, security, and safety.

19. My lab's research aims to uncover personal data collection, sharing, and usage in the online advertising ecosystem.

20. In addition to my research, I regularly teach undergraduate and graduate courses on computer networks and computer security, including special topics courses covering emerging trends in online advertising and tracking.

21. I have received several awards and distinctions for my research. I am a recipient of the Caspar Bowden Award - Runner-up for Outstanding Research in Privacy Enhancing Technologies (2024), Chancellor's Fellowship (2022-2023), Dean's Scholar Award (2020), National Science Foundation CAREER Award (2018), and Fitch-Beach Outstanding Graduate Research Award (2013).

22. I have co-authored more than 100 peer-reviewed research papers. I received the Best Paper Award at the 2023 ACM Internet Measurement Conference for my research on tracking, profiling, and ad targeting in the Amazon Alexa ecosystem. I also received the 2018 Andreas Pfitzmann Award at the Privacy Enhancing Technologies Symposium for my research on designing a system to detect advertising and tracking data flows in mobile apps. I also received the Best Paper Award at the 2017 ACM Internet Measurement Conference for my research on identifying and investigating the abuse of a security vulnerability in Facebook Graph API's implementation of third-party apps. I also received the Best Paper Award at the 2012 IEEE International Conference on Network Protocols for my research on reverse-engineering proprietary network protocols through network traffic analysis.

23. I am the editor-in-chief of the Proceedings on Privacy Enhancing Technologies (PoPETs). I am on the steering committee of the Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb). I am the general chair of the Workshop on Technology and Consumer Protection (ConPro). In the past, I have served as the program chair for the Workshop on Technology and Consumer Protection (ConPro 2022 and 2023) and the Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb 2022 and 2023).

24. My complete CV is attached as **Appendix A**.

IV. BACKGROUND OF RELEVANT TECHNOLOGY

A. Overview of Pixels

25. The term pixel (also known as tracking pixel, web bug, pixel tag, or web beacon) refers to a piece of code (e.g., JavaScript[4] or HTML[5]) or image (e.g., a 1x1 GIF[6]) that is used to track browsing activity on the web.

26. A pixel typically allows a third party[7] (i.e., a domain[8] or origin[9] that is distinct from the first-party website that a website visitor navigates to) to track a website visitor visiting website$_1$ at time$_1$, website$_2$ at time$_2$, and so on. Pixels can track more fine-grained activity on and across websites, such as full webpage URLs,[10] webpage title, search terms, forms fields, adding an item to cart, etc.

27. TikTok internally describes the general concept of pixel [redacted]:

[redacted]

[4] https://developer.mozilla.org/en-US/docs/Web/JavaScript.

[5] https://developer.mozilla.org/en-US/docs/Web/HTML.

[6] Ruohonen, J. and Leppänen, V., 2018, January. *Invisible pixels are dead, long live invisible pixels!*, in Proceedings of the 2018 Workshop on Privacy in the Electronic Society (pp. 28-32).

[7] https://web.dev/learn/privacy/third-parties.

[8] https://developer.mozilla.org/en-US/docs/Glossary/Domain.

[9] https://developer.mozilla.org/en-US/docs/Glossary/Origin.

[10] https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Web_mechanics/What_is_a_URL.

[redacted][11]

28. A pixel is designed to collect two types of data in HTTP[12] request[13] transmissions from a website visitor's web browser to the pixel's web server: (1) identifiers and (2) browsing activity.

a. Identifiers are typically collected via (i) the cookies[14] stored in the web browser's storage[15] and (ii) the combination of IP address[16] and user agent[17] in the transmission from a website visitor's web browser to the pixel's web server.[18] Cookies containing identifiers typically store a 128 bit Universally Unique IDentifier (UUID)[19] that is sufficient for unique identification. There are two main types of cookies: first-party and third-party. First-party cookies are set on the same domain as the visited website's domain. Third-party cookies are set on a different domain as the visited website's domain. Pixels set third-party cookies that allow them to track users across websites. Since some web browsers have now started to restrict third-party cookies, pixels now also set first-party cookies[20] (a practice

[11] TIKTOK-BG-000003014 (emphasis in original).

[12] https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview.

[13] https://developer.mozilla.org/en-US/docs/Web/HTTP/Messages#http_requests.

[14] https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies.

[15] Web browsers support several cookie-like storage mechanisms such as cookies, session storage, local storage, cache storage, and IndexedDB. See https://developer.mozilla.org/en-US/docs/Learn/JavaScript/Client-side_web_APIs/Client-side_storage for more details.

[16] https://developer.mozilla.org/en-US/docs/Glossary/IP_Address.

[17] https://developer.mozilla.org/en-US/docs/Glossary/User_agent.

[18] IAB Tech Lab Identity Solutions Guidance Version 1.0 https://iabtechlab.com/wp-content/uploads/2024/05/Identity-Solutions-Guidance-FINAL.pdf.

[19] https://datatracker.ietf.org/doc/html/rfc4122.

[20] Cookies or their equivalent storage mechanisms such as local storage or session storage.

known as cookie ghostwriting[21,22]) on the same domain as the visited website's domain to circumvent third-party cookie blocking.[23] First-party cookies are used by pixels for both same-site and cross-site tracking.[24,25] The combination of IP address and user agent typically contains sufficiently distinguishing information[26] (quantified in terms of entropy bits[27,28,29,30]) to be used as a unique identifier.[31] This practice of combining IP address, user agent, and other distinguishing browser or device information for identification is also known as fingerprinting.[32]

---

[21] Sanchez-Rola, I., Dell'Amico, M., Balzarotti, D., Vervier, P.A. and Bilge, L., 2021, May. Journey to the center of the cookie ecosystem: Unraveling actors' roles and relationships. In 2021 IEEE Symposium on Security and Privacy (SP) (pp. 1990-2004). IEEE.

[22] Nikkhah Bahrami, P., Fass, A. and Shafiq, Z., 2024. COOKIEGUARD: Characterizing and Isolating the First-Party Cookie Jar. arXiv e-prints, pp.arXiv-2406.

[23] Munir, S., Siby, S., Iqbal, U., Englehardt, S., Shafiq, Z. and Troncoso, C., 2023, November. CookieGraph: Understanding and Detecting First-Party Tracking Cookies. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (pp. 3490-3504).

[24] Munir, S., Lee, P., Iqbal, U., Shafiq, Z. and Siby, S., 2023. PURL: Safe and Effective Sanitization of Link Decoration. arXiv e-prints, pp.arXiv-2308.

[25] Bekos, P., Papadopoulos, P., Markatos, E.P. and Kourtellis, N., 2023, April. The Hitchhiker's guide to facebook web tracking with invisible pixels and click IDs. In Proceedings of the ACM Web Conference 2023 (pp. 2132-2143).

[26] https://clearcode.cc/blog/adtech-id-solutions/ ("A universal ID is a unique user ID that allows AdTech companies to identify users across different websites and devices. Universal IDs are created using **probabilistic data** (e.g. IP address, browser type and model, and user-agent string) or **deterministic data** (e.g. an email address or phone number), or both, to produce an ID." (emphasis in original)).

[27] Eckersley, P. (2010). How unique is your web browser?. In Privacy Enhancing Technologies: 10th International Symposium, PETS 2010, Berlin, Germany, July 21-23, 2010.

[28] Wagner, I. and Eckhoff, D., 2018. Technical privacy metrics: a systematic survey. ACM Computing Surveys, 51(3).

[29] Google. Introducing the Privacy Budget, https://www.youtube.com/watch?v=0STgfjSA6T8&t=423s.

[30] https://github.com/mikewest/privacy-budget/blob/4e5f78adde92bd622dafeceae78682fc0823c0eb/faq.md.

[31] IP address also encodes information about the location of a user. There are numerous IP geolocation services that can estimate the country, state, city, postal code, and even approximate longitude and latitude from IP address. For example, see https://www.maxmind.com/en/geoip-web-services-demo.

[32] Yen, T.F., Xie, Y., Yu, F., Yu, R.P. and Abadi, M., 2012, February. Host Fingerprinting and Tracking on the Web: Privacy and Security Implications. In Network and Distributed System Security (NDSS) Symposium.

b. Browsing activity is collected via the (i) URL,[33] (ii) Referer[34] and Origin[35] headers, or (iii) payload[36] of the transmission from a website visitor's web browser to the pixel's web server. The URL may contain information about the webpage's content (e.g., name of a product) in a query parameter.[37,38] The Referer and Origin headers typically contain the name of the website visited by the website visitor. The payload may contain much more detailed content information[39] such as the detailed description of a product in a standardized format such as JSON,[40] which is a widely used way to store data in a standard human-readable text format that is also amenable to automated machine parsing.

29. The data collected by a pixel is typically used to target website visitors with ads that are personalized based on their browsing history. For example, a website visitor whose browsing history indicates interest in hiking may receive targeted ads for hiking poles.[41] After a personalized ad is served, pixels are also used to collect information about whether a website visitor viewed or clicked on an ad and ended up buying the advertised product.[42] This information is then used to further personalize ads. For example, a website visitor may get a personalized ad

[33] https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Web_mechanics/What_is_a_URL.

[34] https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referer.

[35] https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Origin.

[36] https://developer.mozilla.org/en-US/docs/Glossary/Payload_body.

[37] https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Web_mechanics/What_is_a_URL#parameters.

[38] URL parameters may also contain identifiers such as cookies, email address, or phone number.

[39] Payload may also contain identifiers such as cookies, email address, or phone number.

[40] https://developer.mozilla.org/en-US/docs/Glossary/JSON.

[41] https://clearcode.cc/glossary/ad-targeting/.

[42] https://clearcode.cc/glossary/conversion-pixel/.

for a hiking pole that they saw in an ad and added to cart but did not buy yet. In addition, and [redacted], the data collected by a pixel can be used to improve various related systems such as fraud detection[43] and user identification and targeting algorithms.[44]

B. Overview of TikTok Pixel

30. TikTok Pixel is JavaScript source code that is embedded on non-TikTok websites. TikTok also describes the TikTok Pixel as: "TikTok Pixel is a piece of code that you can place on your website that allows you to share website events with TikTok."[45]

31. TikTok Pixel's source code is written by TikTok and is served by TikTok's server. The website developers of the non-TikTok websites[46] that use the Pixel do not write the source code, nor can they directly modify it.

32. TikTok instructs website developers that TikTok Pixel [redacted][47] This is to ensure that the TikTok Pixel is [redacted].[48] As discussed later in Section V.B in more detail, the TikTok Pixel's placement in the [redacted].

[43] https://clearcode.cc/blog/rtb-online-advertising-fraud/.

[44] IAB Tech Lab. Identity Solutions Guidance Version 1.0, https://iabtechlab.com/wp-content/uploads/2024/05/Identity-Solutions-Guidance-FINAL.pdf.

[45] https://ads.tiktok.com/help/article/tiktok-pixel.

[46] Because websites that use the TikTok Pixel typically advertise their products and services on the TikTok app or web platform, TikTok's internal documents commonly refer to these non-TikTok websites as [redacted]

[47] TIKTOK-BG-000008579 at -586.

[48] https://www.corewebvitals.io/pagespeed/head-vs-footer-javascript-and-core-web-vitals.

33. According to TikTok's own public documentation,[49, 50] the data collected by TikTok Pixel includes at least the following: "Timestamp,"[51] "Cookies,"[52] "IP Address,"[53] "User Agent,"[54] "Ad/Event information,"[55] and "Metadata & Button Clicks."[56,57]

34. TikTok Pixel collects this data through "standard events" and "custom events":

a. Standard events include "Add Payment Info," "Add to Cart," "Add to Wishlist," "Click Button," "Complete Payment," "Complete Registration," "Contact," "Download," "Initiate Checkout," "Place an Order," "Search," "Submit Form," "Subscribe," and "View Content."[58]

b. Custom events are "actions that TikTok partners can define themselves beyond the predefined standard events list."[59]

[49] https://ads.tiktok.com/help/article/tiktok-pixel.

[50] One internal document also states that the following constitutes [redacted] TIKTOK-BG-000157260, at -262; *see also* TIKTOK-BG-8008 at -010 [redacted]

[51] https://ads.tiktok.com/help/article/tiktok-pixel ("Used to determine when website actions took place, like when a page was viewed or when a product was purchased").

[52] *Id.* ("Used to help with the measurement, optimization, and targeting of your campaigns. First-party cookies are optional, but third-party cookies are on by default with the TikTok Pixel. Performance is boosted when first- and third-party cookies are paired with Advanced matching").

[53] *Id.* ("Used to determine the geographic location of an event").

[54] *Id.* ("Used to determine the device make, model, operating system, and browser information").

[55] *Id.* ("Information about the ad a person on TikTok has clicked on or an event that was initiated").

[56] *Id.* ("Includes descriptive page metadata, structured microdata, page performance data, and button clicks").

[57] As discussed below, TikTok Pixel also automatically collects Page URL and Referrer URL by default. Notably, URL is missing from TikTok's public documentation about what data TikTok Pixel collects.

[58] https://ads.tiktok.com/help/article/supported-standard-events; *see also* TIKTOK-BG-000000128.

[59] TIKTOK-BG-000000128.

35. In addition to these standard and custom events, TikTok, by default, collects data through the "PageView" event, which TikTok also refers to as [redacted][60] TikTok Pixel, by default, "will always include page view events which measure when a person lands on any of your webpages."[61] TikTok's internal documents and deposition testimony also [redacted]

36. The scale of TikTok Pixel's data collection is staggering. According to multiple independent estimates, TikTok Pixel is used by more than 300 thousand websites.[63,64] An April 2023 study on the prevalence of pixels have estimated that the TikTok Pixel is present on 7.41 percent of over 3,100 websites spanning a range of industries, including Financial Services & Banking, Healthcare, Technology and SaaS, e-Commerce, Airlines, and U.S. Federal and State

[60] TIKTOK-BG-000000875 (Depo Ex. 55) at -878 [redacted].

[61] TIKTOK-BG-000000128; *see also* https://web.archive.org/web/20231129091101/https://ads.tiktok.com/help/article/standard-events-parameters?lang=en. At some point after the commencement of this litigation, TikTok removed this disclosure of the default collection of PageView event data from its website.

[62] *See, e.g.*, TIKTOK-BG-000151364 (Depo Ex. 46), at -366 [redacted]; *id.* [redacted]; *id.* at -377 (defining [redacted]; TIKTOK-[redacted]; TIKTOK-BG-000150667 (Depo Ex. 49) [redacted]); *id.* [redacted]; Tr. of Becca Wong Depo. (May 17, 2024) at 133:1-5 [redacted] (objection omitted)); *id.* at 134:24-135:4 ([redacted] (objection omitted)).

[63] https://trends.builtwith.com/websitelist/TikTok-Conversion-Tracking-Pixel/United-States.

[64] https://www.nerdydata.com/reports/tiktok-pixel/de68a0d2-1056-47f0-aec4-6f705982fc81.

Government.[65] Another study dated March 2024 reports that the TikTok Pixel is present on 12 percent of 3,419 websites spanning healthcare, technology, financial services, retail, and sites of companies listed in the S&P 500 index.[66] According to one TikTok internal document dated [redacted], TikTok Pixel [redacted].[67] As stated in another internal document that appears to have been created [redacted][68]

37. The data collected by TikTok Pixel is [redacted][69] In fact, [redacted]. According to an internal document, TikTok [redacted][70] According to another internal document, [redacted][72] As described in Section VIII in more detail, my analysis of the data produced by TikTok similarly shows that the match rate for US data is [redacted] This means that [redacted].

[65] Feroot, "Beware of Pixels & Trackers," 2023 Feroot Client-Side Security Report, Apr. 5, 2023. https://go.feroot.com/hubfs/4605309/Reports/Beware%20of%20Pixels%20&%20Trackers%20-%20Feroot%20Client-Side%20Security%20Report%20March%202023.pdf.

[66] LOKKER, "Website Privacy and Compliance Challenges: Quantifying Website Privacy Risks," Mar. 2024, https://lokker.com/wp-content/uploads/2024/04/LOKKER_Online-Data-Privacy-Report_032024-2.pdf.

[67] TIKTOK-BG-000003014, at -3016.

[68] TIKTOK-BG-000009897 at -897. Yet another document from [redacted] notes that TikTok [redacted] TIKTOK-BG-000157229 at -230.

[69] TIKTOK-BG-000086213 at -214.

[70] TIKTOK-BG-000009897 at -897.

[71] TIKTOK-BG-000005393 at -394 [redacted].

[72] *Id.*

C. Overview of TikTok Events API

38. TikTok Events API allows TikTok to collect [redacted]. [73] The main difference between TikTok Events API and TikTok Pixel is that the former is a "server-to-server" (between website's and TikTok's servers) data-collection mechanism and the latter is "client-to-server" (between website visitor's web browser and TikTok's server) data-collection mechanism.

39. TikTok Events API's "server-to-server" data collection [redacted] [74] and tracking protection features. [75,76,77]

40. TikTok recommends "setting up both TikTok's Events API and Pixel together." [78,79] Therefore, the data collected by them is often duplicative, which is then deduplicated by TikTok. [80]

---

[73] TIKTOK-BG-000082617, at -617; TIKTOK-BG-000086213 at -214.

[74] TIKTOK-BG-000086213 at -214. *See also* TIKTOK-BG-000008579 at -586; TIKTOK-BG-000082696 at -696; TIKTOK-BG-000002238 at -242.

[75] https://stape.io/blog/how-to-set-up-tiktok-events-api ("With server-side tracking, you will be able to collect more events. TikTok events API is resistant to ad blockers, ITPs, and other tracking restrictions.").

[76] https://ads.tiktok.com/help/article/events-api ("**Resilient solutions for an evolving advertising ecosystem:** The Events API together with an existing Pixel ensures a more sustainable transition in response to changes in the advertising industry.").

[77] https://www.tiktok.com/business/en-US/blog/events-api-consolidated-endpoint ("TikTok launches enhanced Events API with consolidated endpoint"); *id.* ("The era of third-party cookies as we know it is ending. Internet users are looking for more control over their data and how it is used. The use of ad blockers and secure web browsers are on the rise as a result. At the same time, US state governments are signing into law new regulations and policies protecting user data and increasing requirements for collecting, sharing and using data (CPRA, CTDPA, VCDPA, etc). Finally, operating systems and browsers are implementing technical and policy changes limiting how data is collected and used. This combination of factors is driving the end of third-party cookies." "To help advertisers better prepare for this cookieless future, we're excited to announce the launch of a consolidated endpoint across Events API for Web, App (in testing), and Offline.").

[78] TIKTOK-BG-000001355 at -355.

[79] https://ads.tiktok.com/help/article/events-api ("we recommend having an Events API integration with your existing Pixel integration to maximize performance benefits"); *id.* ("Use both TikTok's Pixel and Events API together").

[80] https://ads.tiktok.com/help/article/event-deduplication.

41. Just like TikTok Pixel, the data collection by the TikTok Events API is real-time and contemporaneous with the loading of the webpage. Specifically, TikTok recommends sending "**the event in real-time**" and "as soon as it is seen on the advertiser's server" when using TikTok Events API.[81] Thus, even though the data collected by TikTok Events API first goes from the website visitor's web browser to the website's server before reaching TikTok's server, it remains real-time and contemporaneous with the loading of the webpage just like the data collected by TikTok Pixel.

42. Just like TikTok Pixel, TikTok Events API can collect identifiers in cookies as well as IP address and user agent.[82]

43. Just like TikTok Pixel, TikTok Events API can [redacted].[83]

44. Just like TikTok Pixel, the data collected by TikTok Events API is used for advertising and other related systems (as further described in Section VII).[84,85]

---

[81] https://business-api.tiktok.com/portal/docs?rid=p41a33fdhon&id=1771100865818625 ("it's **highly recommended to send the event in real-time (without batching)** as soon as it is seen on the advertiser's server") (emphasis in original).

[82] https://ads.tiktok.com/help/article/how-to-set-up-matching-events-with-events-api (explaining that Events API can be set up to collect and transmit "Click ID," i.e. "[a] unique identifier appended to the URL every time a person clicks on a TikTok ad"; "Email and Phone (Hashing required)"; "External ID (Hashing required)," including "[a]dvertiser-side identifiers, such as loyalty membership IDs, advertiser customer IDs, and external cookie IDs"; "IP Address (IP) and User Agent (UA)" and "1st Party Cookie (if using with Pixel)").

[83] TIKTOK-BG-000001355 at -357; *see also* TIKTOK-BG-000008008 at -010.

[84] https://ads.tiktok.com/help/article/events-api ("TikTok Events API provides advertisers with a reliable connection between TikTok and advertiser's marketing data, across web, app, and offline (eg. Store, CRM) channels with the ability to customize the information they share with TikTok.").

[85] https://www.tiktok.com/business/en-US/blog/events-api-consolidated-endpoint ("Events API is a secure server-to-server (S2S) integration with TikTok that allows advertisers to share marketing data with us in a secure connection directly from their server. By sharing this marketing data with TikTok, advertisers are able to unlock the performance advertising benefits of better optimization and delivery.").

45. While TikTok recommends setting up TikTok Pixel and TikTok Events API together, given that TikTok Events API was launched after TikTok Pixel, the scale of TikTok Events API's data collection [redacted][86] TikTok's internal documents suggest that [redacted][87]

46. Just like with TikTok Pixel, the data collected by TikTok Events API is agnostic to whether a website visitor is a TikTok user or not. In the same vein, [redacted]. According to an internal document from [redacted], [redacted].[88] Thus, just as with TikTok Pixel, [redacted]

V. UNIFORMITY IN TIKTOK PIXEL'S DATA COLLECTION

A. TikTok Pixel Automatically Collects Seven Data Categories with All Events.

47. I use RiteAid's website as a running example of a non-TikTok website from where TikTok Pixel collects data.

48. I use the developer tools[89] that are available in all major web browsers for my testing and analysis. More specifically, I used DevTools[90] that are built into the Chrome browser.

[86] TIKTOK-BG-000003172 at -175.

[87] TIKTOK-BG-000003172 at -175.

[88] TIKTOK-BG-000003172 at -176.

[89] https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Tools_and_setup/What_are_browser_developer_tools.

[90] https://developer.chrome.com/docs/devtools.

I opened a new guest profile[91] in Chrome browser with no existing cookies or other browser state and navigated to the homepage of RiteAid's website.[92]

49. As shown in Figure 1, I used the "Sources" panel in Chrome browser's DevTools to investigate all resources, including source code, that are loaded on RiteAid's website. Three JavaScript source code files from TikTok's analytics.tiktok.com server are loaded on RiteAid's website. The three JavaScript source code files are named main.MWY1ZWZmZjM0MQ.js, identify_ce1d8843.js, and events.js. The first two files are the general files that are typically the same across any website with TikTok Pixel. The last file named events.js is unique to RiteAid as indicated by the "sdkid=C2IOKVFMU8QAJ3JEQ61G" query parameter after the file name. "C2IOKVFMU8QAJ3JEQ61G" is the unique identifier of the TikTok Pixel on RiteAid.

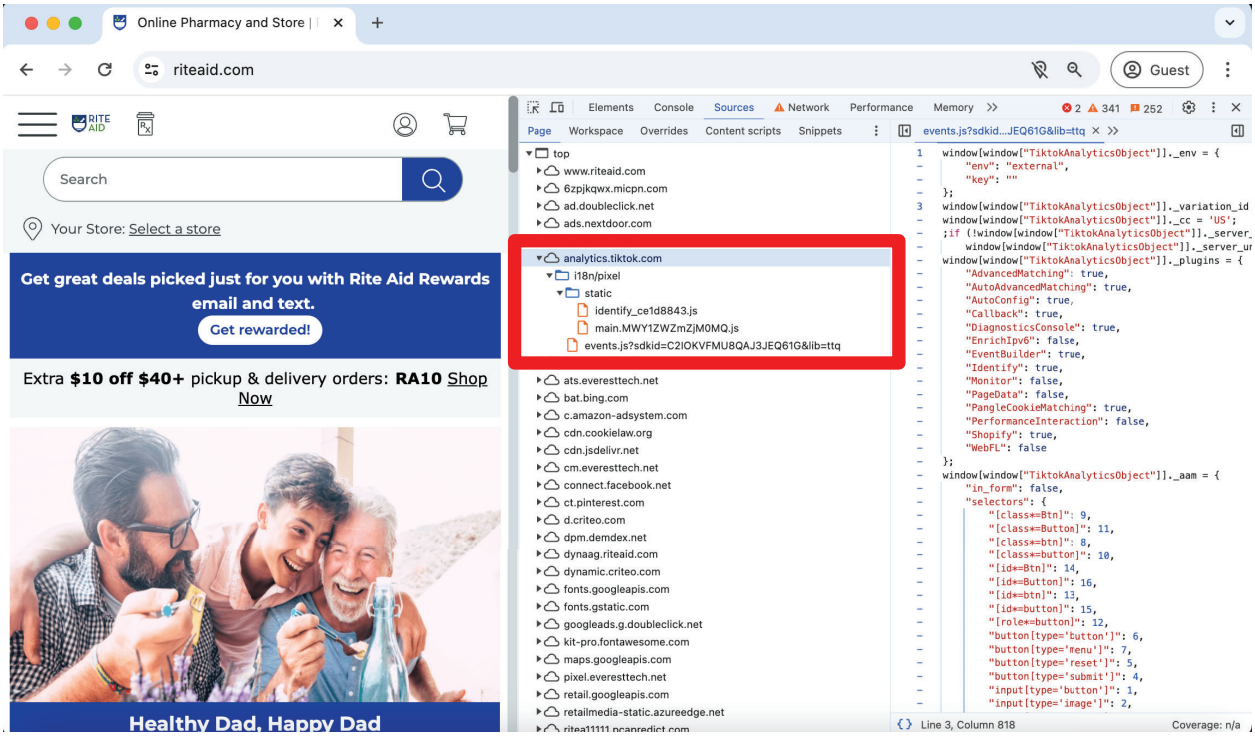


Figure 1: TikTok Pixel source code loaded on the homepage of RiteAid's website

[91] https://support.google.com/chrome/answer/6130773.

[92] https://www.riteaid.com/.

50. As shown in Figure 2, I then used the "Network" panel[93] in Chrome browser's DevTools to investigate the transmissions from the web browser to TikTok's server. The figure lists five transmissions to TikTok. The first three are GET [94] requests to download the aforementioned three JavaScript source code files. The next two are POST[95] requests that send data to TikTok's server: one POST request sends data to https://analytics.tiktok.com/api/v2/pixel and the other POST request sends data to https://analytics.tiktok.com/api/v2/pixel/act.

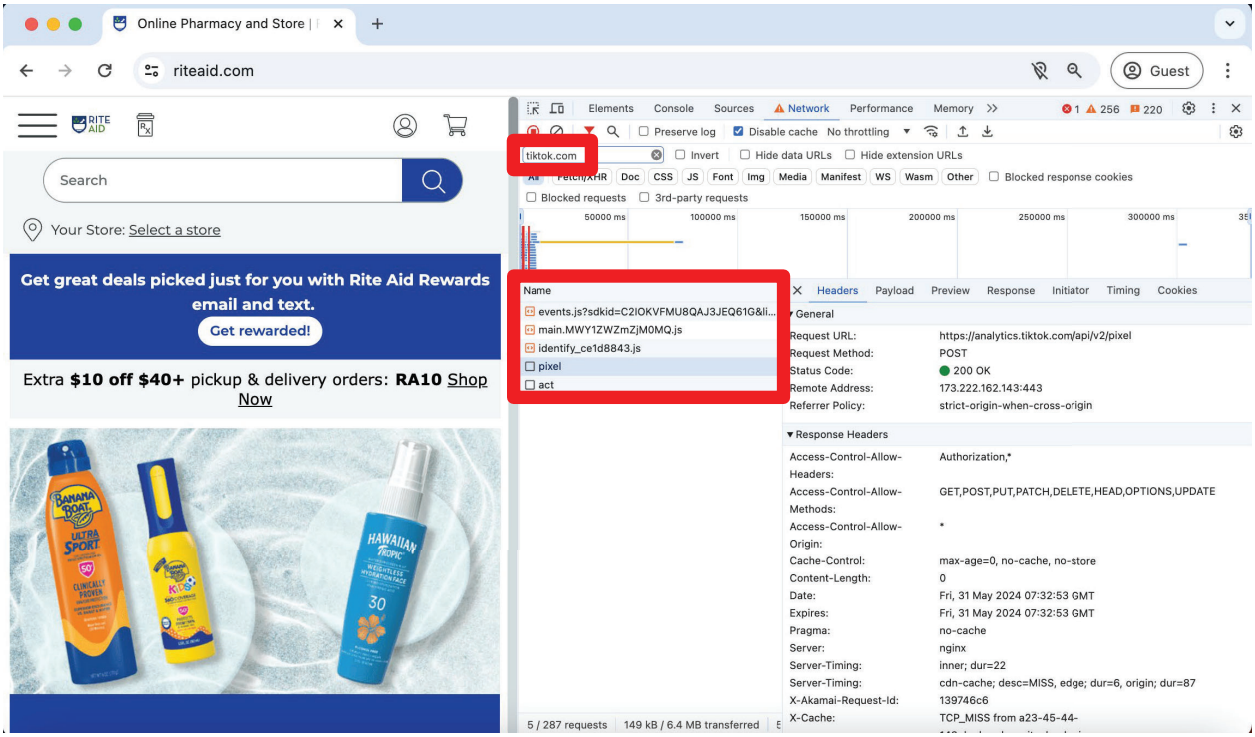


Figure 2: GET and POST transmissions to TikTok's server on the homepage of RiteAird's website

51. As shown in Figure 3, the payload of the first POST request to https://analytics.tiktok.com/api/v2/pixel includes a JSON object with several key-value pairs for "Pageview" event. This JSON object includes fields such as event, message_id, timestamp,

[93] https://developer.chrome.com/docs/devtools/network.

[94] https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/GET.

[95] https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/POST.

context.page.url, context.page.referrer, context.user.userAgent, context.user.anonymous_id, context.session_id, etc. In addition to these fields in the JSON object, the transmission includes _ttp third-party cookie in the Cookie header of the POST request and IP address in the source address field of the network layer header.

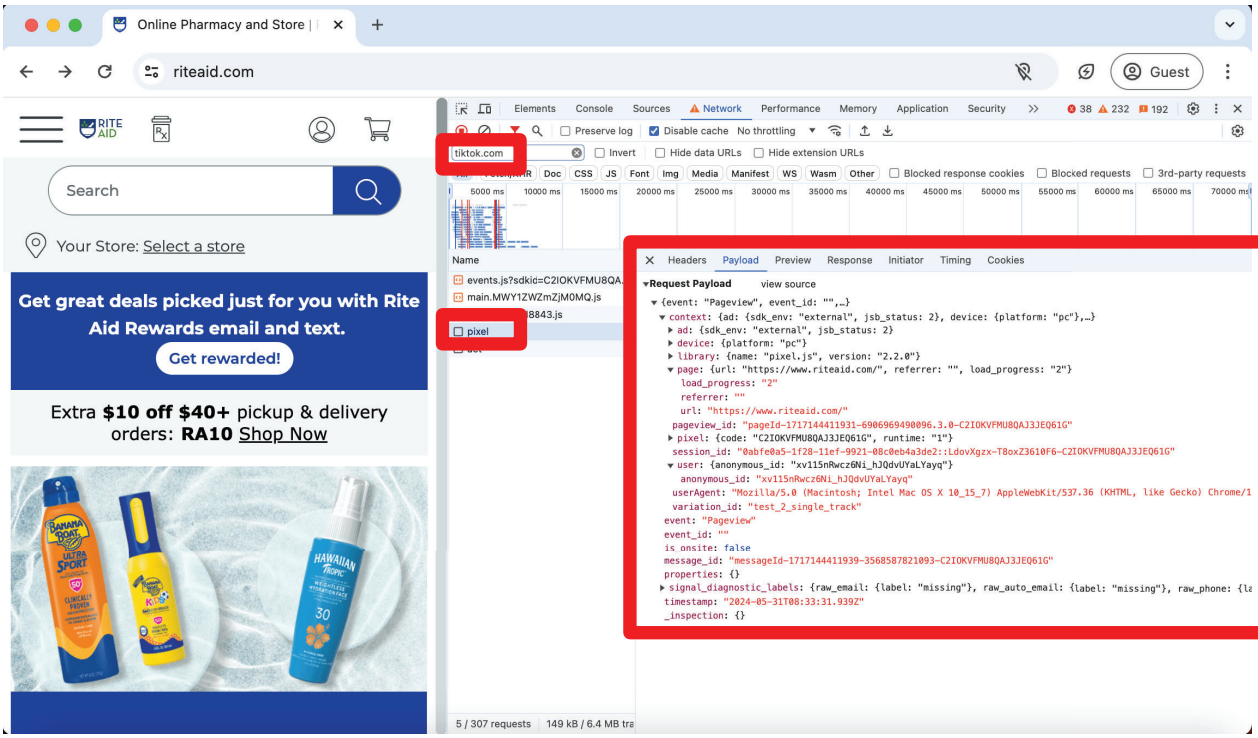


Figure 3: JSON payload of a POST transmission to TikTok's server on the homepage of RiteAid's website

52. As shown in Figure 4, the payload of the second POST request to https://analytics.tiktok.com/api/v2/pixel/act also includes a JSON object with several key-value pairs for the "Metadata" action corresponding to the same "PageView" event. This JSON object includes fields such as action, message_id, timestamp, context.page.url, context.page.referrer, context.user.userAgent, context.user.anonymous_id, context.session_id, auto_collected_properties.page_trigger, auto_collected_properties.content_data.json_ld, auto_collected_properties.content_data.meta, auto_collected_properties.content_data.microdata, auto_collected_properties.content_data.open_graph, etc. In addition to these fields in the JSON

object, the transmission includes _ttp third-party cookie in the Cookie header of the POST request and IP address in the source address field of the network layer header.

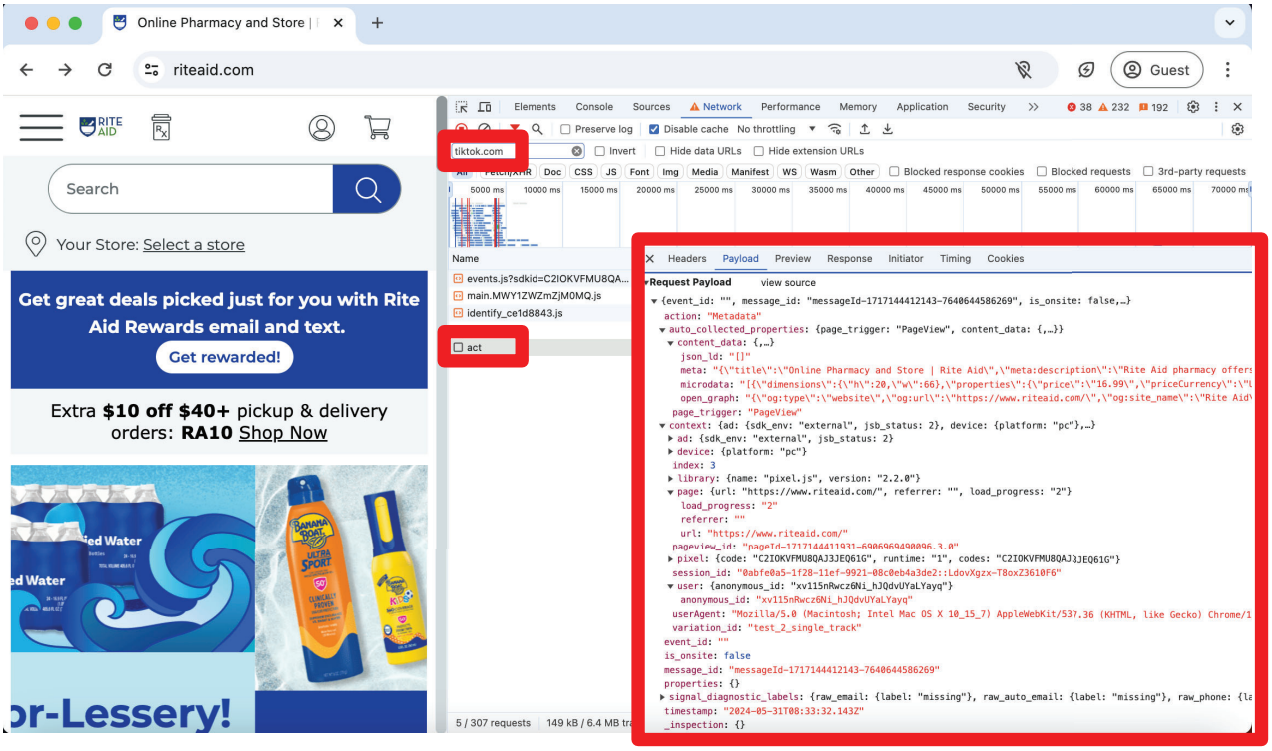


Figure 4: JSON payload of a POST transmission to TikTok's server on the homepage of RiteAid's website

53. As shown in Figure 5, I then navigated to the "Sexual Wellness" subpage on RiteAid's website and the same five transmissions to TikTok's server are observed, including the two POST requests for the "PageView" event and the "Metadata" action corresponding to the same "PageView" event. The POST request to https://analytics.tiktok.com/api/v2/pixel/act shown in Figure 5 includes a JSON object with several key-value pairs for the "Metadata" action corresponding to the same "PageView" event. This JSON object includes the same fields as described above. Additionally, the auto_collected_properties.content_data.meta field includes the webpage's title ("Sexual Health and Wellness Products | Family Planning | Rite Aid") and the context.page.url field contains the full page URL ("https://www.riteaid.com/shop/sexual-wellness?page=2").

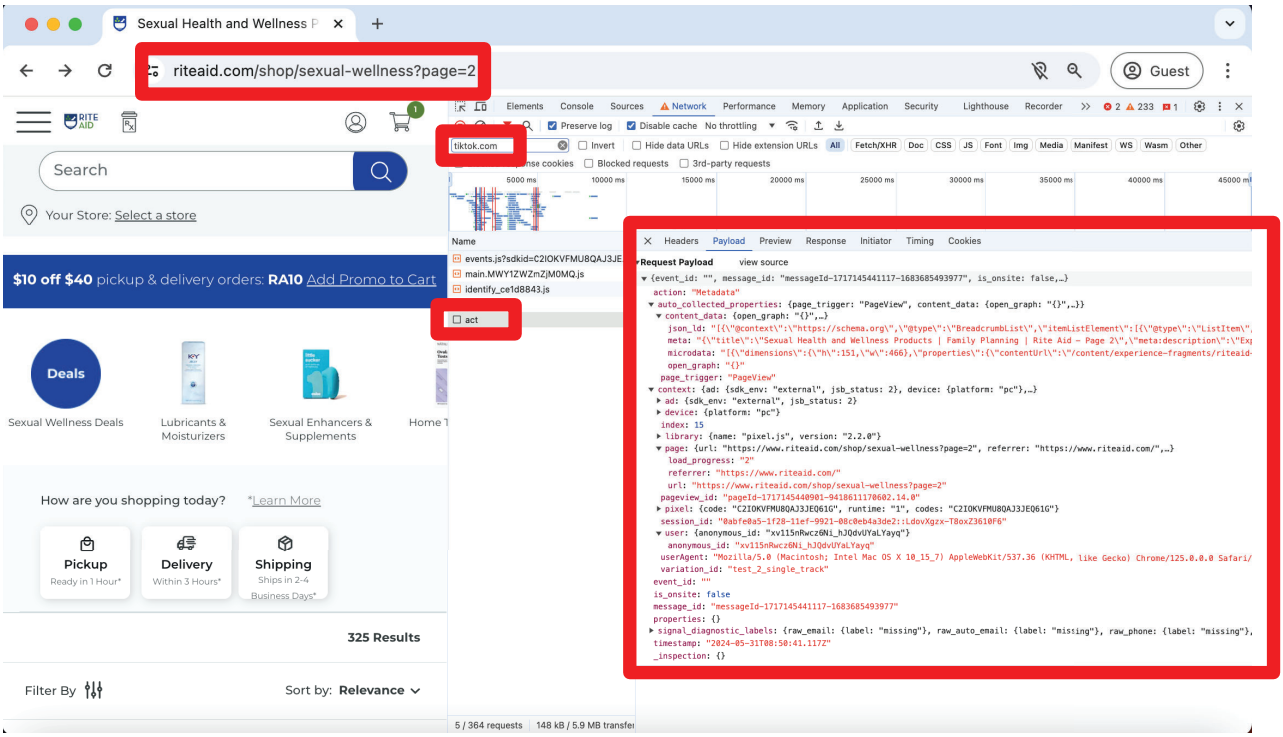


Figure 5: JSON payload of a POST transmission to TikTok's server on a subpage of RiteAid's website

54. As shown in Figure 6, I then clicked to add an emergency contraceptive product to cart, which results in another POST request containing information about the fact that I performed a "Click" action on a add-to-cart button on the sexual wellness subpage. The POST request to https://analytics.tiktok.com/api/v2/pixel/act shown in Figure 6 includes a JSON object with several key-value pairs for the "Click" action. This JSON object mostly includes the same fields as described earlier, but it includes fields such as auto_collected_properties.page_trigger, auto_collected_properties.trigger_element.inner_text, and auto_collected_properties.trigger_element.attributes.class that contain information about the content of the button on which I clicked.

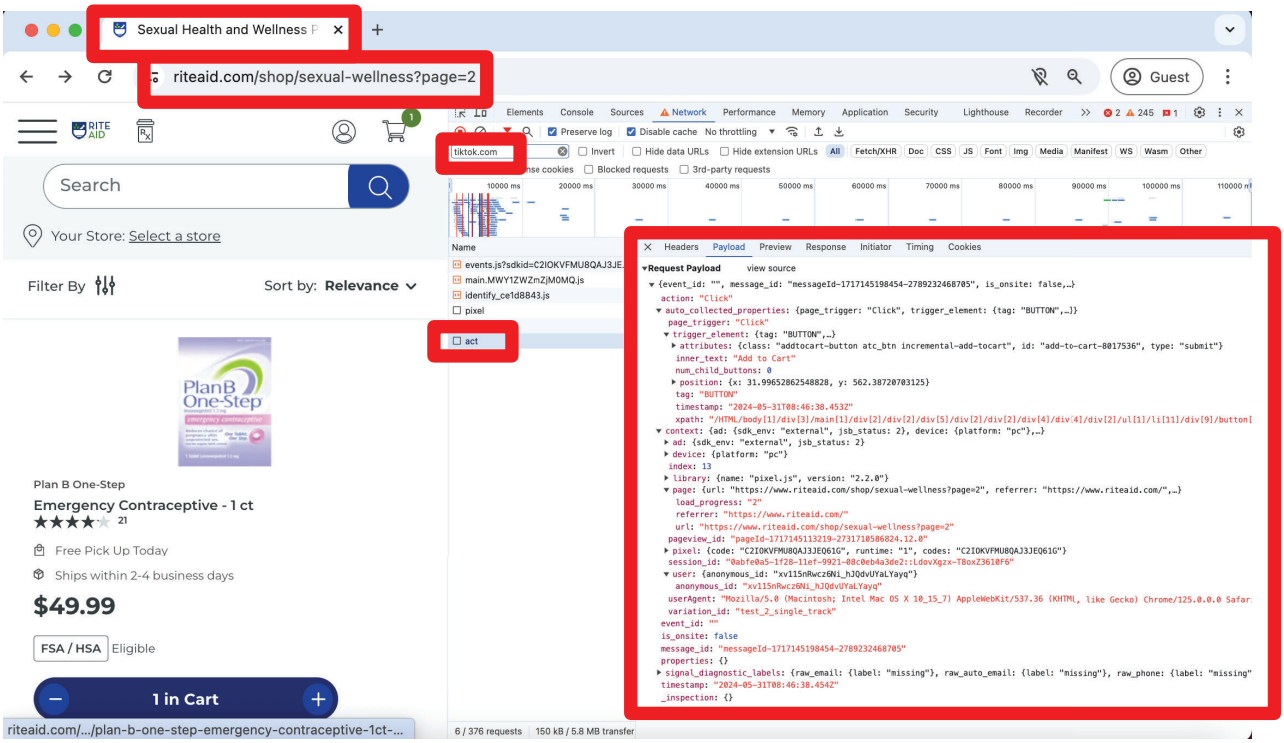


Figure 6: JSON payload of a POST transmission to TikTok's server on a subpage of RiteAid's website

55. As shown in Figure 7, I then clicked on the Plan B One-Step emergency contraceptive product, which results in another POST request containing information about the fact that I performed a "Click" action on the specific product with URL https://www.riteaid.com/shop/plan-b-one-step-emergency-contraceptive-1ct-8017536. The POST request to https://analytics.tiktok.com/api/v2/pixel/act shown in Figure 7 includes a JSON object with several key-value pairs for the "Click" action. This JSON object mostly includes the same fields as described earlier, but it includes fields such as auto_collected_properties.trigger_element.attributes.destination that contains the full URL of the Plan B One-Step emergency contraceptive product webpage.

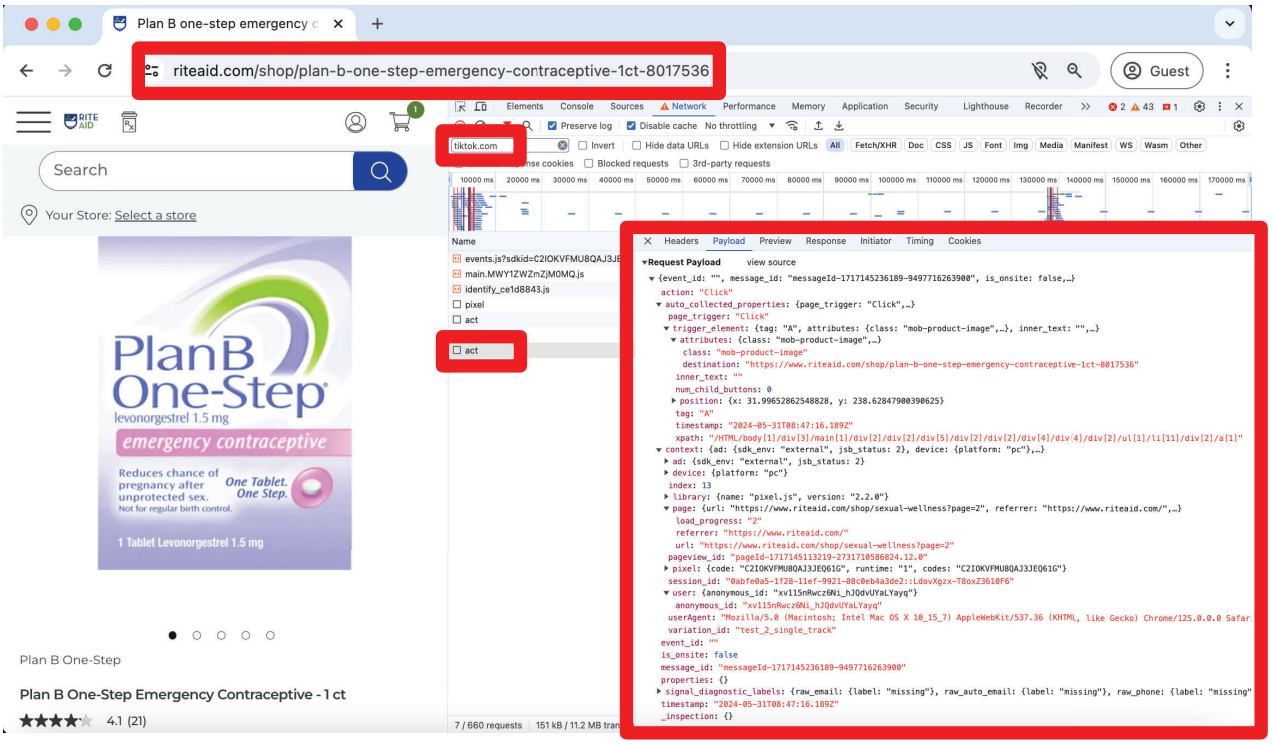


Figure 7: JSON payload of a POST transmission to TikTok's server on a subpage of RiteAid's website

56. Based on this testing and similar testing that I have conducted on various websites where TikTok Pixel is deployed, I conclude that TikTok Pixel automatically collects information about the precise sequence of actions performed by a website visitor on a website through a series of POST requests corresponding to various events, including the default "PageView" event.

57. Overall, I conclude that TikTok Pixel automatically collects the following seven categories of data for all events, including the default "PageView" event: (a) Timestamp; (b) IP Address; (c) User Agent; (d) Cookies; (e) URL; (f) Event Information; and (g) Content Information.

58. I elaborate on each of these seven categories of data automatically collected by the TikTok Pixel below.

59. **Timestamp**: TikTok Pixel automatically collects the exact timestamp in every POST request.

i. The timestamp is collected at the millisecond (1/1000 of one second) granularity in the "timestamp" field in the payload of the POST request.

ii. The timestamp value is in the ISO 8601 standard format [96] such as 2024-05-31T11:13:01.351Z. 2024-05-31 is the date portion, in the format YYYY-MM-DD. Here, 2024 is the year, 05 is the month (May), and 31 is the day of the month. T is a delimiter that separates the date and time components. 11:13:01.351 is the time portion, where 11 is the hour, 13 is the minutes, 01.351 is the seconds with millisecond precision. Z indicates that the time is in Coordinated Universal Time (UTC), meaning no time zone offset is applied. The Z stands for "Zulu" time, which is another term for UTC.

iii. On its publicly available website, TikTok states that the Pixel collects timestamp information in order "to determine when website actions took place, like when a page was viewed or when a product was purchased."[97]

60. **IP Address**: TikTok Pixel automatically collects IP Address, which is a "number used to address each device on an IP network uniquely,"[98] in the source address field of the network layer header of the POST request. TikTok states that it uses the IP address to determine the website visitor's geographic location.[99]

61. **User Agent**: TikTok Pixel automatically collects User Agent, which is a string that encodes information to identify the operating system, vendor, browser, and the browser version[100] in the "userAgent" field in the payload of the POST request. TikTok states that it uses the User

[96] https://www.iso.org/iso-8601-date-and-time-format.html.

[97] https://ads.tiktok.com/help/article/tiktok-pixel.

[98] https://developer.mozilla.org/en-US/docs/Glossary/IP_Address.

[99] https://ads.tiktok.com/help/article/tiktok-pixel (TikTok explaining that the IP Address is "used to determine the geographic location of an event").

[100] https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/User-Agent.

Agent to determine the website visitor's device, operating system, and browser.[101] For example "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36" tells[102] TikTok that the website visitor's device is a MAC computer with operating system 10.15.7 and Chrome browser version 121. The combination of the IP Address and User Agent is widely used in the industry as an identifier.[103] TikTok is [redacted]. More specifically, TikTok's [redacted][104]

62. **Cookies**: TikTok Pixel automatically collects three different types of cookies containing identifiers: (1) session ("tt_sessionId" stored in the browser's session storage that is collected in the "session_id" field in the payload of the POST request), (2) first-party ("_ttp" first-party cookie, that is ghostwritten[105,106] by TikTok Pixel on the website's domain [redacted][107] and collected in the "anonymous_id" field in the payload of the POST request), and (3) third-party ("_ttp" third-party cookie set on the tiktok.com domain, even

[101] *See* https://ads.tiktok.com/help/article/tiktok-pixel.

[102] https://explore.whatismybrowser.com/useragents/parse/#parse-useragent.

[103] https://clearcode.cc/blog/adtech-id-solutions/.

[104] TIKTOK-BG-000150406 (Depo Ex. 52); *see also* Tr. of Becca Wong Depo. (May 17, 2024) at 187:5-14 ("[redacted] (objections omitted)).

[105] Sanchez-Rola, I., Dell'Amico, M., Balzarotti, D., Vervier, P.A. and Bilge, L., 2021, May. Journey to the center of the cookie ecosystem: Unraveling actors' roles and relationships. In 2021 IEEE Symposium on Security and Privacy (SP) (pp. 1990-2004). IEEE.

[106] Munir, S., Siby, S., Iqbal, U., Englehardt, S., Shafiq, Z. and Troncoso, C., 2023, November. CookieGraph: Understanding and Detecting First-Party Tracking Cookies. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (pp. 3490-3504).

[107] TIKTOK-BG-000009045 at -047 [redacted]

though the website visitor may never have directly visited tiktok.com, is collected in the Cookie header field of the POST request). These three cookies contain identifiers that are used by TikTok to track the website visitor browsing activity on a particular website and across different websites. The ability to identify a person on and across a large number of different websites using cookies allows TikTok to obtain a significant coverage of a person's browsing history[108] and infer private and sensitive attributes such as gender, age, location, ethnicity and race, sexual orientation, and political orientation.[109, 110] TikTok states in its public documentation that "Cookies help the measurement, optimization and targeting of your campaigns."[111] TikTok further states in an internal document that cookies are [redacted][112] TikTok internally recognizes[113] that [redacted]; they are [redacted]. [114] First-party cookies [redacted].[115] TikTok encouraged advertisers to leave

[108] Englehardt, S. and Narayanan, A., 2016, October. Online tracking: A 1-million-site measurement and analysis. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 1388-1401).

[109] Hinds, J. and Joinson, A.N., 2018. What demographic attributes do our digital footprints reveal? A systematic review. PloS one, 13(11), p.e0207112.

[110] Englehardt, S., Reisman, D., Eubank, C., Zimmerman, P., Mayer, J., Narayanan, A. and Felten, E.W., 2015, May. Cookies that give you away: The surveillance implications of web tracking. In Proceedings of the 24th International Conference on World Wide Web (pp. 289-299).

[111] https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel.

[112] TIKTOK-BG-000008616 at -618.

[113] TIKTOK-BG-000000835 at -838 and -839.

[114] *Id.*; *see also* TIKTOK-BG-000000853 (Depo Ex. 65) at -857 and -858.

[115] TIKTOK-BG-000000853 (Depo Ex. 65) at -860 (noting that [redacted]).

[redacted]. [116]

63. **Uniform Resource Locator ("URL")**: TikTok Pixel automatically collects two different types of URLs by default: (1) Page URL and (2) Referrer URL.

i. The Page URL collected in the "page.url" field of the POST request is the full URL of the webpage that the visitor is viewing. The Referrer URL collected in the "page.referrer" field of the POST request is the full URL of the preceding webpage from which the website visitor navigated to the current webpage.

ii. The URLs collected by TikTok can contain both (a) personally identifying and (b) sensitive information, typically in the URL parameters[117] that are always collected by TikTok Pixel in both Page and Referrer URLs.

iii. URLs can contain personal identifiers such as name, date of birth, gender, phone number, email, and address in URL parameters automatically collected by TikTok Pixel.

iv. URLs can contain sensitive content, including sensitive search queries. For instance, when a website visitor searches for "pregnancy test" on riteaid.com, the following Page URL is collected by TikTok containing URL parameter "q" whose value includes the search term: https://www.riteaid.com/shop/catalogsearch/result/?q=pregnancy%20test.

[116] *Id.* at -859 ([redacted]); Tr. of Becca Wong Depo. (May 17, 2024) at 257:18-22 ("Q. [redacted] (objection omitted)); *id.* at [redacted]

[117] https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Web_mechanics/What_is_a_URL#parameters.

In other words, through the URL, TikTok receives information that the website visitor searched riteaid.com for pregnancy tests. Similarly, when a website visitor clicks on an emergency contraceptive product, the following URL is collected by TikTok containing the product information: https://www.riteaid.com/shop/plan-b-one-step-emergency-contraceptive-1ct-8017536. In other words, TikTok receives information that the website visitor visited the "Plan B One-Step Emergency Contraceptive" product page on riteaid.com. Of course, this information is accompanied by all the other automatically sent identifiers discussed above, including IP Address, User Agent, and Cookies.

v. As shown through the various examples below, TikTok's sample of the non-TikTok user data produced in discovery confirms that [redacted]. Specifically, the sample URLs listed below, which I understand TikTok collected in less than an hour on just one day of its choosing (March 28, 2024) ("March 28 Sample Data"),[118] demonstrate [redacted]. One URL reveals that [redacted] Another URL reveals how a website visitor [redacted] Yet other URLs identify website visitors [redacted]. In the March

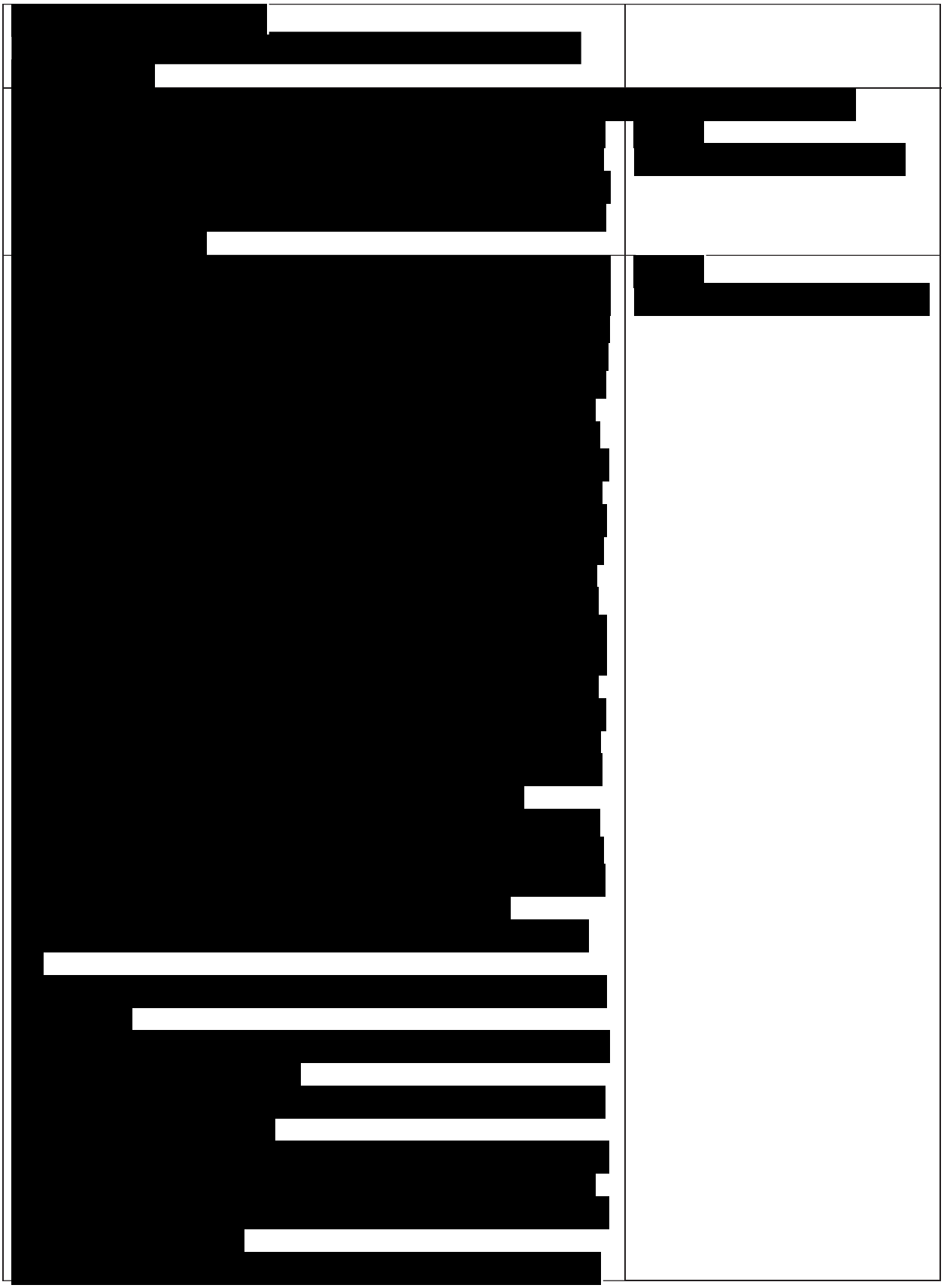
[118] TIKTOK-BG-0124043.

28 Sample Data alone, I counted [redacted] [redacted][119]

URL Collected by TikTok Pixel[120]	[redacted] Included in URL
[redacted]	[redacted]

[119] [redacted] further explained: A value of "[redacted] Feb. 27, 2024 Email from Defendants' Counsel K. Yin to Plaintiffs' Counsel G. Park.

[120] Note that "%20" in a URL denotes a space; and "%40" in a URL denotes the symbol "@". https://www.tutorialspoint.com/html/html_url_encoding.htm.



[redacted]

vi. TikTok's March 28 Sample Data [redacted] shown through the examples below, these [redacted]

URL Collected by TikTok Pixel[121]	[redacted] Included in URL
[redacted]	

vii. Once again, the above URLs were contained within a fraction of the data that TikTok collected via the Pixel—from under one hour on March 28, 2024. It can reasonably be

[121] Note that the search term follows "q=" in the URL.

inferred that a wider sample of collected data would contain additional amounts of personally identifying and sensitive information.

64. **Event Information**: TikTok Pixel automatically collects information about standard and custom events in the POST requests. This category of information includes the name of the event in the field "event" (e.g., "PageView," "AddToCart"), name of the associated action in the field "action" (e.g., "Click"), and a unique identifier of the event or action in the "message_id" field of the POST request. Even if the website has not configured any such events, however, TikTok Pixel collects event information for at least the default PageView event. TikTok explains that the default PageView event means that [redacted][122]

65. **Content Information**: TikTok Pixel automatically collects data about content of the webpage in the POST requests. Content information typically includes substantive information about the webpage's content that a website visitor is viewing, including the title of a webpage, the description of a webpage as well as the product or item name, category, and identifier. Notably, the TikTok Pixel scans for and scrapes or infers this content information without websites having to configure any settings to pass this data to TikTok.

i. For the default PageView event, TikTok Pixel automatically collects properties of the webpage content in four standard formats: (1) JSON-LD[123] in the "json_ld" field,

[122] TIKTOK-BG-000151574 (Depo Ex. 47), at -576; *see also supra* at nn.60-62 and accompanying text.

[123] https://json-ld.org/ ("**Linked Data** Linked Data empowers people that publish and use information on the Web. It is a way to create a network of standards-based, machine-readable data across Web sites. It allows an application to start at one piece of Linked Data, and follow embedded links to other pieces of Linked Data that are hosted on different sites across the Web."); *id.* ("**JSON-LD** JSON-LD is a lightweight Linked Data format. It is easy for humans to read and write. It is based on the already successful JSON format and provides a way to help JSON data interoperate at Web-scale. JSON-LD is an ideal data format for programming environments, REST Web services, and unstructured databases such as Apache CouchDB and MongoDB.").

(2) Meta [124] in the "meta" field, (3) Microdata [125] in the "microdata" field, and (4) OpenGraph [126] in the "open_graph" field. Put simply, these are four standard machine-readable ways in which webpage content is typically described to search engines and crawlers. TikTok Pixel automatically collects this content information from the HTML of the webpage in the "content_data" field in the POST request. For example, as discussed earlier in this section, on the Sexual Wellness subpage on RiteAid's website, the "content_data" field in the POST request to TikTok's server includes webpage title "Sexual Health and Wellness Products | Family Planning | Rite Aid" and description "Explore our extensive selection of sexual health and wellness products online including sex toys, games, contraceptives & more. Orders over $34.99 ship free." As another example of specific product pages, the "content_data" field collected by TikTok Pixel includes product name and additional details such as "Benadryl Allergy, 25 mg, Ultratabs - 24 tablet box | Rite Aid," "Benadryl Ultratabs

[124] https://www.w3schools.com/tags/tag_meta.asp ("The <meta> tag defines metadata about an HTML document. Metadata is data (information) about data. <meta> tags always go inside the <head> element, and are typically used to specify character set, page description, keywords, author of the document, and viewport settings. Metadata will not be displayed on the page, but is machine parsable. Metadata is used by browsers (how to display content or reload page), search engines (keywords), and other web services.").

[125] https://developer.mozilla.org/en-US/docs/Web/HTML/Microdata ("Microdata is part of the WHATWG HTML Standard and is used to nest metadata within existing content on web pages. Search engines and web crawlers can extract and process microdata from a web page and use it to provide a richer browsing experience for users. Search engines benefit greatly from direct access to this structured data because it allows search engines to understand the information on web pages and provide more relevant results to users. Microdata uses a supporting vocabulary to describe an item and name-value pairs to assign values to its properties. Microdata is an attempt to provide a simpler way of annotating HTML elements with machine-readable tags than the similar approaches of using RDFa and classic microformats.").

[126] https://ogp.me/ ("To turn your web pages into graph objects, you need to add basic metadata to your page. We've based the initial version of the protocol on RDFa which means that you'll place additional <meta> tags in the <head> of your web page. The four required properties for every page are: og:title - The title of your object as it should appear within the graph, e.g., 'The Rock'. og:type - The type of your object, e.g., 'video.movie'. Depending on the type you specify, other properties may also be required. og:image - An image URL which should represent your object within the graph. og:url - The canonical URL of your object that will be used as its permanent ID in the graph, e.g., 'https://www.imdb.com/title/tt0117500/'.").

Antihistamine Allergy Medicine Tablets - 24 ct," price "product:price:amount\":\"6.99," and even detailed reviews ("Benedryl is the best for relieving immediate allergy symptoms. I take one after I cut the grass to calm the sneezing and itching").

ii. For all other standard and custom events, TikTok Pixel automatically collects properties of the webpage content in fields such as "content_name," "content_category," and "content_id." For example, for the AddToCart event for an Allergy medication on RiteAid (https://www.riteaid.com/shop/benadryl-allergy-25-mg-ultratabs-24-tablets-0033202), TikTok Pixel collects "Benadryl Ultratabs Antihistamine Allergy Medicine Tablets - 24 ct," "Medicine & Health/Allergy & Sinus/Allergy Medicine," and "0033202"[127] for the aforementioned three fields.

iii. TikTok collects this content data through at least two discrete mechanisms: Pixelbot and Enhance Data Postback. TikTok's internal documents describe [redacted]"[128] It "[redacted]"[129] It's [redacted]"[130] [redacted]."[131]

[127] "0033202" is the catalog identifier of the product on RiteAid's website. *See* https://www.riteaid.com/shop/catalogsearch/result/?q=0033202.

[128] TIKTOK-BG-000132449.

[129] TIKTOK-BG-000132448.

[130] TIKTOK-BG-000149005 at -006.

[131] *Id.*

iv. In the past, TikTok publicly disclosed the existence of the Pixelbot on its website.[132] At some point, after the commencement of this litigation, TikTok appears to have removed this public disclosure notwithstanding the fact that the TikTok Pixel continues to automatically collect Content Information.

v. A second tool with which the Pixel automatically collects Content Data is through a feature called Enhance Data Postback. On TikTok's website, TikTok describes its automatic collection of content data through Enhance Data Postback as follows: "TikTok is improving the functionality of pixels by collecting and using landing page information such as metadata and button clicks. This new information will, in the future, enable TikTok to provide recommendations on how to enhance your pixel event setup and even offer automated solutions. This data may also be used to personalize ad campaigns for people on TikTok and improve TikTok's ad delivery systems."[133] "With this update," TikTok continues, "the TikTok Pixel will send the following information from your webpage where a TikTok Pixel is installed:

- Structured microdata from supported formats like JSON-LD/Schema.org and Opengraph.
- Descriptive page metadata (for example, page titles, product information, key parameters such as value and currency).
- Page performance data (for example, page load times).

[132] *See* TIKTOK-BG-000000257 (TikTok's website as of August 15, 2023, after the commencement of litigation, describing that "TikTok Pixel automatically scans and analyzes keywords on your public website to help classify and contextualize your content. . . . TikTok Pixel uses web crawling protocols that respect standard robots.txt rules. In order for your website to be scanned, the TikTok Pixel must be installed.").

[133] https://ads.tiktok.com/help/article/enhance-data-postback-with-the-tiktok-pixel.

- Button click text and elements (for example, button name, descriptive text, and attributes)."[134]

vi. This auto-collection of metadata and button clicks is consistent with TikTok's internally articulated goals of [redacted].[135] As one former TikTok employee testified, TikTok sought to [redacted][136]

66. These seven categories of data are automatically collected, and its collection either cannot be disabled at all by the websites or is turned on by default. Where a default option can be toggled off, discovery shows that websites [redacted]. For example, in response to Interrogatory 9 asking TikTok to identify "every Website that has left in place the default configuration of the TikTok SDK to allow First-Party Cookies," TikTok responded with a [redacted] As discussed later in Section V.D, my own analysis [redacted] shows that nearly all websites keep the default configuration of the TikTok Pixel to allow first-party cookies.

[134] *Id.*

[135] *See* TIKTOK-BG-000009006 (Depo Ex. 54), at -026; *see also id.* at -027 [redacted].

[136] Tr. of Becca Wong Depo. (May 17, 2024) at 204:23-205:4.

[137] TIKTOK-BG-000007829.

B. TikTok Pixel's Data Collection Happens in Real Time and Contemporaneously with the Loading of Webpages.

67. TikTok Pixel's data collection relies on a browser feature called "event listeners,"[138] which ***listen*** to various "events"[139] (distinct from the standard and custom events in TikTok Pixel's vocabulary) occurring in the website visitor's web browser in real-time and contemporaneous with the loading of the webpage.

68. Specifically, TikTok Pixel's source code[140] contains instructions to set up listeners for events such as "mousedown,"[141] "pointerdown,"[142] "mouseup,"[143] "pointerup,"[144]

[138] https://developer.mozilla.org/en-US/docs/Web/API/EventTarget/addEventListener.

[139] https://developer.mozilla.org/en-US/docs/Web/API/Event ("An event can be triggered by the user action e.g. clicking the mouse button or tapping keyboard, or generated by APIs to represent the progress of an asynchronous task."); *id.* ("Many DOM elements can be set up to accept (or 'listen' for) these events, and execute code in response to process (or 'handle') them. Event-handlers are usually connected (or 'attached') to various HTML elements (such as <button>, , , etc.) using EventTarget.addEventListener(), and this generally replaces using the old HTML event handler attributes.").

[140] https://analytics.tiktok.com/i18n/pixel/static/main.MWY1ZWZmZjM0MQ.js.

[141] https://developer.mozilla.org/en-US/docs/Web/API/Element/mousedown_event ("The mousedown event is fired at an Element when a pointing device button is pressed while the pointer is inside the element.").

[142] https://developer.mozilla.org/en-US/docs/Web/API/Pointer_events ("Pointer events are DOM events that are fired for a pointing device. They are designed to create a single DOM event model to handle pointing input devices such as a mouse, pen/stylus or touch (such as one or more fingers).").

[143] https://developer.mozilla.org/en-US/docs/Web/API/Element/mouseup_event ("The mouseup event is fired at an Element when a button on a pointing device (such as a mouse or trackpad) is released while the pointer is located inside it.").

[144] https://developer.mozilla.org/en-US/docs/Web/API/Pointer_events ("Pointer events are DOM events that are fired for a pointing device. They are designed to create a single DOM event model to handle pointing input devices such as a mouse, pen/stylus or touch (such as one or more fingers).").

"mousemove,"[145] "pointermove,"[146] "keydown,"[147] and "click."[148] The listeners set up by TikTok Pixel are instantaneously (i.e., in real-time and without any delay) triggered when these events occur during the webpage load, allowing TikTok Pixel to intercept movement of the mouse or any other pointer device, when keys are pressed, and when buttons are clicked as well as content information (e.g., using browser features such as window.location.href[149] to intercept the page URL, document.referrer[150] to intercept the referrer URL, and document.querySelectorAll[151] to intercept webpage content in JSON-LD, Meta, Microdata, and OpenGraph formats) while it is in-transit from the website visitor's browser to the website's server. Thus, TikTok Pixel's event listeners assist with its interception of Content Information.

---

[145] https://developer.mozilla.org/en-US/docs/Web/API/Element/mousemove_event ("The mousemove event is fired at an element when a pointing device (usually a mouse) is moved while the cursor's hotspot is inside it.").

[146] https://developer.mozilla.org/en-US/docs/Web/API/Pointer_events ("Pointer events are DOM events that are fired for a pointing device. They are designed to create a single DOM event model to handle pointing input devices such as a mouse, pen/stylus or touch (such as one or more fingers).").

[147] https://developer.mozilla.org/en-US/docs/Web/API/Element/keydown_event ("The keydown event is fired when a key is pressed.").

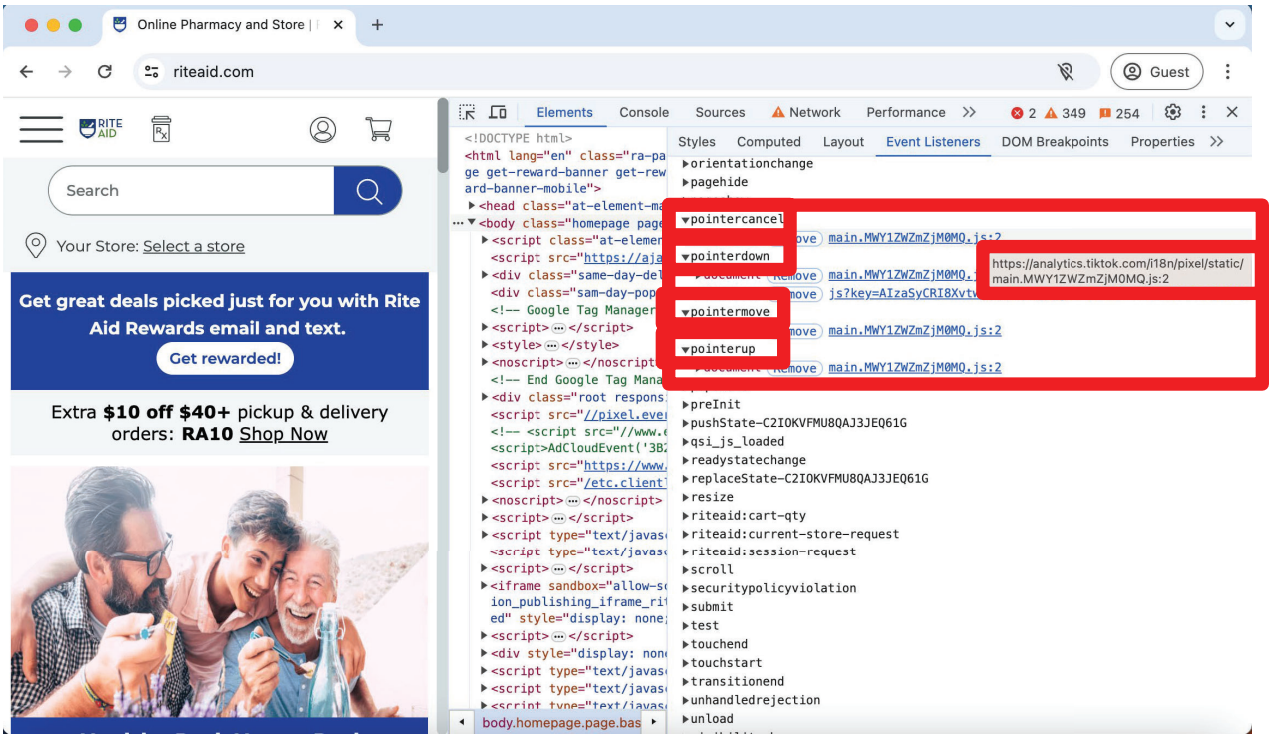
[148] https://developer.mozilla.org/en-US/docs/Web/API/Element/click_event ("An element receives a click event when any of the following occurs • a pointing-device button (such as a mouse's primary button) is both pressed and released while the pointer is located inside the element. • a touch gesture is performed on the element • the Space key or Enter key is pressed while the element is focused").

[149] https://developer.mozilla.org/en-US/docs/Web/API/Window/location ("The Window.location read-only property returns a Location object with information about the current location of the document. Though Window.location is a read-only Location object, you can also assign a string to it. This means that you can work with location as if it were a string in most cases: location = 'http://www.example.com' is a synonym of location.href = 'http://www.example.com'.") TikTok Pixel source code (https://analytics.tiktok.com/i18n/pixel/static/main.MWY1ZWZmZjM0MQ.js) uses window.location to intercept the URL of the webpage.

[150] https://developer.mozilla.org/en-US/docs/Web/API/Document/referrer ("The Document.referrer property returns the URI of the page that linked to this page.").

[151] https://developer.mozilla.org/en-US/docs/Web/API/Document/querySelector ("The Document method querySelector() returns the first Element within the document that matches the specified selector, or group of selectors. If no matches are found, null is returned."). TikTok Pixel source code (https://analytics.tiktok.com/i18n/pixel/static/main.MWY1ZWZmZjM0MQ.js) uses querySelectorAll to intercept content information such as JSON-LD.

69. As shown in Figure 8, I used the "Elements" panel[152] in Chrome browser's DevTools to investigate the event listeners installed by TikTok Pixel source code on RiteAid's website. The "Event Listeners" panel[153] shows that the TikTok Pixel source code installed event listeners for click and pointer events.



[152] https://developer.chrome.com/docs/devtools/elements.

[153] https://developer.chrome.com/blog/easily-jump-to-event-listeners.

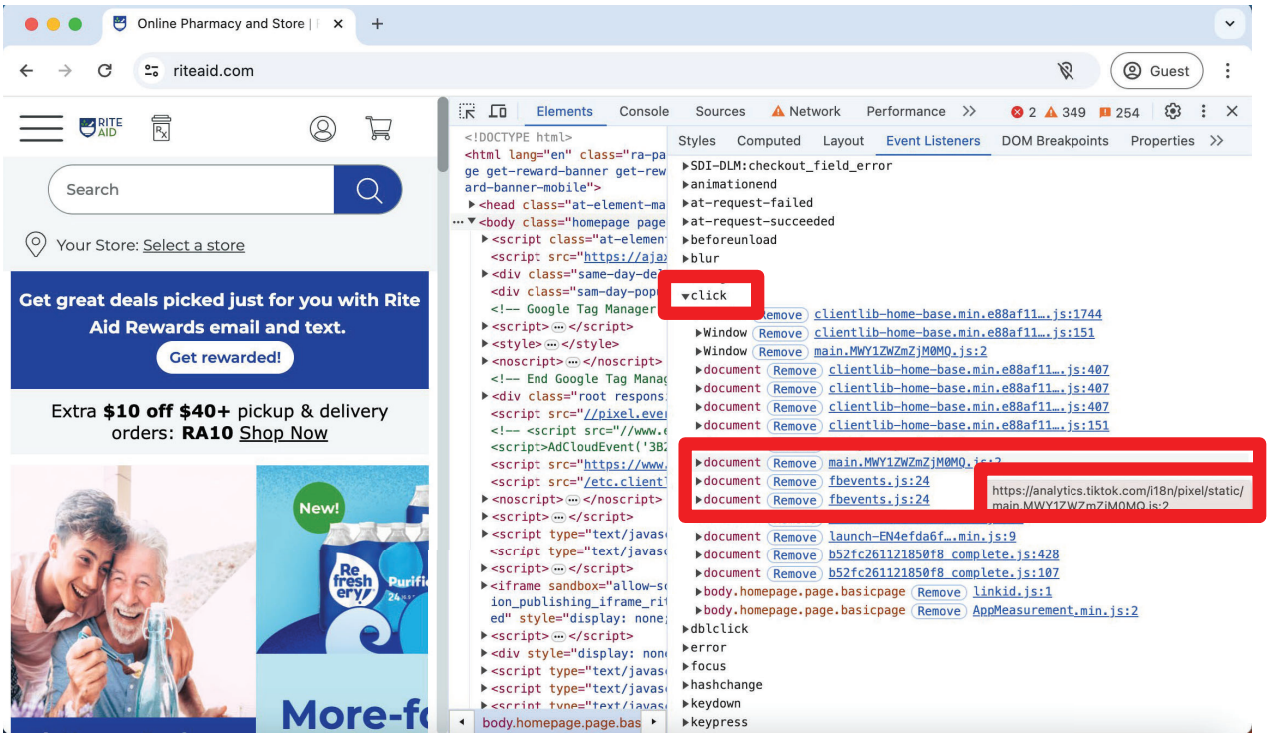


Figure 8:TikTok Pixel sets up event listeners in a website visitor's web browser to intercept Content Information

70. As explained earlier in Section IV.B, TikTok [redacted] .[154] The header section comes before the main body section of webpages, which means that TikTok Pixel source code is loaded and ready for data collection (e.g., through the aforementioned "listeners") as soon as a website visitor visits a webpage. Thus, TikTok collects the data even if the website visitor navigates away from the webpage before the page finishes loading in the browser completely. TikTok's internal documentation confirms that the [redacted] "[155]

[154] TIKTOK-BG-000008579 at -586.

[155] TIKT
19 ("[redacted]" (objections omitted)).

71. Figure 9 plots the timeseries of the transmissions from the web browser to servers when RiteAid's website is loaded. The red lines indicate the five transmissions (three to download JavaScript source code files and two POST requests for the "PageView" event and the "Metadata" action corresponding to the same "PageView" event) from the web browser to TikTok server. The blue lines indicate the transmissions from the web browser to other servers. It is evident that the transmissions containing the seven categories of data to the TikTok server occur contemporaneously with the loading of the webpage.

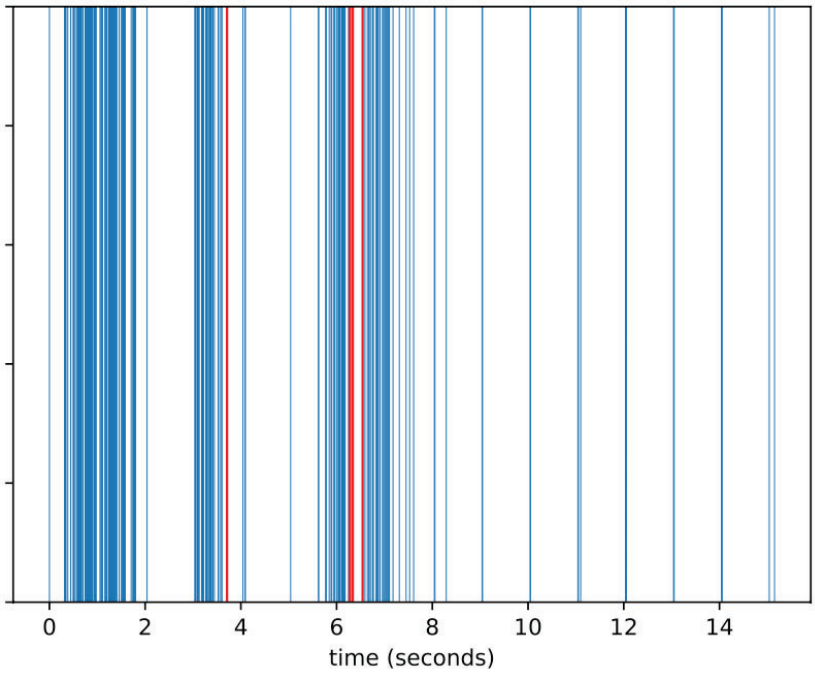


Figure 9:Timeseries of transmissions when RiteAid's website is loaded (*red lines represent the transmissions to TikTok's server*)

C. TikTok Pixel Consumes Measurable Storage and Compute Overhead.

72. As shown in Figure 10, I used the "Network" panel[156] in Chrome browser's DevTools investigate the storage and compute overhead of TikTok Pixel.

[156] https://developer.chrome.com/docs/devtools/network/reference.

73. The "Size" column lists the size in bytes of each transmission from the web browser to TikTok's server. Note that the size of the three JavaScript source code files of TikTok Pixel are approximately 147 kilobytes. The size of each POST request sent to TikTok server is approximately 0.7-0.8 kilobytes. The total size of TikTok Pixel source code and POST requests on this webpage is approximately 149 kilobytes.[157]

74. The "Time" column[158] lists the time in milliseconds it takes to complete each transmission from the web browser to TikTok's server. The total time it took for all five transmissions on this webpage is 424 milliseconds. Note that this time is computed on a powerful MacBook Pro M2 Max laptop with a high-speed WiFi network that achieved 100+ megabyte upload and download throughput and < 10 millisecond idle latency.[159] Thus, this time is likely the lower bound of the time it would take on a less-powerful consumer device on a medium-quality household broadband Internet connection.[160]

[157] Beyond the the source code and POST requests, TikTok Pixel also downloads and stores identifiers and other data in cookies and session storage that occupy approximately 110 bytes. This information can be seen in the "Application" panel (https://developer.chrome.com/docs/devtools/application) in Chrome browser's DevTools.

[158] https://developer.chrome.com/docs/devtools/network/reference/?utm_source=devtools#timing-explanation.

[159] Tested using Speedtest by Ookla https://www.speedtest.net/result/16322271776.

[160] https://www.fcc.gov/consumers/guides/household-broadband-guide.

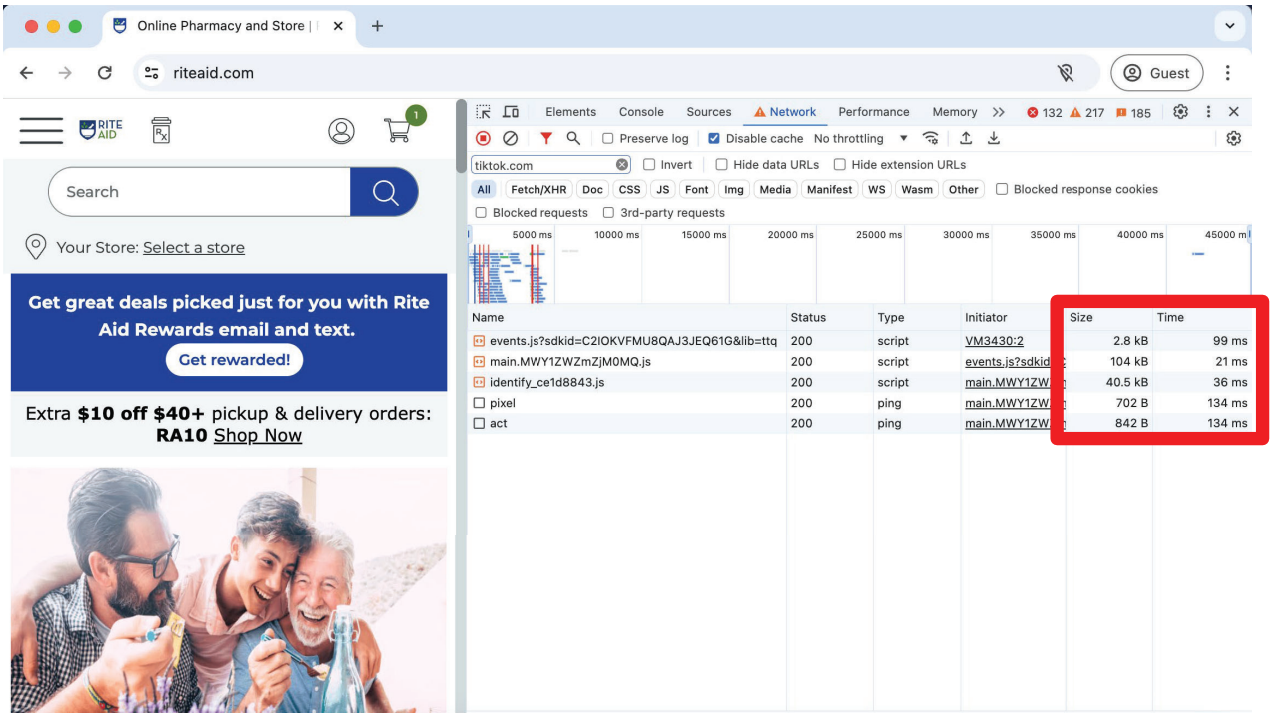


Figure 10: Storage (Size) and Compute (Time) consumed by TikTok Pixel on a website visitor's device

75. TikTok's own measurements are [redacted], one TikTok employee wrote that [redacted][161] According to the employee, the TikTok Pixel [redacted]

D. TikTok Pixel's Data Collection Is Uniform.

a. *There Is No Substantial Variability in TikTok Pixel's Default Data Collection Across Websites.*

76. I have been asked by counsel to investigate whether there is substantial variability in TikTok Pixel's data collection across different websites.

[161] TIKTOK-BG-000157392 at -397.

[162] *Id.*

77. I investigate the variability in TikTok Pixel's data collection across different websites in two ways:

- I crawled a random sample of websites from processed data produced by TikTok (TIKTOK-BG-0124043). To this end, I first compiled the list of unique website domains from that document and then randomly sampled a URL associated for each randomly sampled domain. Each URL was crawled using a fresh Chrome browser (version 125) instance in its default setting that was automated using ChromeDriver[163] (configured to simulate a website visitor that simply loads the webpage and does not engage in any interaction on the webpage such as click on any cookie disclosure or consent banners) and the network traffic logs were collected using ChromeDriver's built-in logging feature.[164] For each sample, I analyzed the network traffic logs to confirm that there are transmissions to TikTok's server (analytics.tiktok.com). This is to ensure that TikTok Pixel is deployed on the URL. This process continued until there were 1,000 URLs, each with a TikTok Pixel transmission. The source code of my crawls and the list of these 1,000 "Random Sample" URLs are provided in **Appendix B**.
- Separately, I crawled top-ranked websites in a list of websites produced by TikTok (TIKTOK-BG-000002788), identified as having used the TikTok Pixel.[165] To this end, I first compiled the list of unique website domains and then identified the top-ranked

[163] https://developer.chrome.com/docs/chromedriver.

[164] https://developer.chrome.com/docs/chromedriver/logging/performance-log.

[165] Tr. of 30(b)(6) Branky Shao Depo. (June 7, 2024) at 272:3-24 [redacted]").

domains using the Tranco[166] ranking. For each domain, a randomly selected URL from sample processed data produced by TikTok (TIKTOK-BG-0124043) was crawled using a fresh Chrome browser (version 125) instance in its default setting that was automated using ChromeDriver[167] (configured to simulate a website visitor that simply loads the webpage and does not engage in any interaction on the webpage such as click on any cookie disclosure or consent banners) and the network traffic logs were collected using ChromeDriver's built-in logging feature.[168] For each sample, I analyzed the network traffic logs to confirm that there are transmissions to TikTok's server (analytics.tiktok.com). This is again to ensure that TikTok Pixel is deployed on the URL. This process continued until there were 1,000 URLs, each with a TikTok Pixel transmission. The source code of my crawls and the list of these 1,000 "Top-Ranked" URLs are provided in **Appendix B**.

[166] Pochat, V.L., Van Goethem, T., Tajalizadehkhoob, S., Korczyński, M. and Joosen, W., 2018. Tranco: A research-oriented top sites ranking hardened against manipulation. arXiv preprint arXiv:1806.01156.

[167] https://developer.chrome.com/docs/chromedriver.

[168] https://developer.chrome.com/docs/chromedriver/logging/performance-log.

78. The following table reports the percentage of the 1,000 "Random Sample" and 1,000 "Top-Ranked" URLs where each of the seven data categories are collected by TikTok. It is evident that there is no substantial variability in TikTok Pixel's collection of the seven data categories across both (random sample and top-ranked) sets of websites.

	Random Sample	Top-Ranked
Timestamp	100.0%	100.0%
IP Address	100.0%	100.0%
User Agent	100.0%	100.0%
Cookies[169]	100.0%	100.0%
URL[170]	100.0%	100.0%
Event Information[171]	100.0%	100.0%
Content Information[172]	98.0%	97.2%

79. The small fraction of websites from which TikTok Pixel does not collect Content Information either do not have the webpage set up using one of the machine-readable formats supported by TikTok Pixel or have toggled off the default Enhance Data Postback.[173] The former case represents a scenario where TikTok Pixel attempted to collect Content Information but was unable to due to the website's formatting. Thus, the results in the above table are a lower bound of the webpages where TikTok Pixel attempts to collect the seven data categories. The latter case can be automatically detected and excluded from analysis if necessary.[174]

[169] Third-party cookie, First-party cookie, or Session ID.

[170] Page URL or Referrer URL.

[171] Event or Message ID.

[172] content_data or properties.

[173] https://ads.tiktok.com/help/article/enhance-data-postback-with-the-tiktok-pixel.

[174] A corner case that I found and handled was that TikTok Pixel sent data in a GET request rather than a POST request.

80. It is important to recognize that the percentages reported here are on a per-webpage basis, not on a per-user basis. This distinction is important because the probability that there exists a website visitor for whom TikTok has not collected all categories of data is practically zero. To elaborate, as reflected in the above table, the probability that TikTok Pixel does not collect Content Information on one webpage is 2.8%, on any of two webpages is 0.8%, and on any of three or more webpages is 0.0%.[175] Given that TikTok Pixel collects data on hundreds of thousands of websites and a non-TikTok user (or class member) would have visited many websites over the Class Period,[176,177] I can conclude that TikTok Pixel has collected Content Information from 100% of class members.

b. There Is No Substantial Variability in TikTok Pixel's Default Data Collection Across Different Web Browsers.

81. I have been asked by counsel to investigate whether there is substantial variability in TikTok Pixel's data collection across different web browsers.

82. I investigate the variability in TikTok Pixel's data collection across different web browsers in two ways:

- I crawled six websites[178] included in the Second Amended Complaint using four major web browsers (Chrome, Safari, Edge, Firefox) that, combined, account for more than 95% of the browser market share in the United States.[179] For each of the six websites visited, I navigated to the homepage, conducted a search on that homepage if that was an option, and

[175] Ross, S.M., 2014. Introduction to probability models. Academic press.

[176] https://trends.builtwith.com/websitelist/TikTok-Conversion-Tracking-Pixel/United-States.

[177] https://www.nerdydata.com/reports/tiktok-pixel/de68a0d2-1056-47f0-aec4-6f705982fc81.

[178] The six websites are buildabear.com, etsy.com, hulu.com, riteaid.com, upwork.com, and vitaminshoppe.com.

[179] https://gs.statcounter.com/browser-market-share/all/united-states-of-america. My testing focuses on the default settings of the web browsers.

clicked on one subpage. Other than search or clicking on a subpage, I did not interact with any cookie disclosure or consent banners, if available. Each webpage was crawled using a fresh browser[180] instance in its default setting, and the network traffic logs were collected using each browser's respective developer tools. The underlying data, containing further details about my crawls, is provided in **Appendix B**.

- Separately, I analyzed the processed data produced by TikTok (TIKTOK-BG-0124043[181]) across the four major web browsers (Chrome, Safari, Edge, Firefox) that together account for more than 95% of the browser market share in the United States.[182] This analysis covers TikTok Pixel's data collection on tens of thousands of data points for a diverse range of web browser configurations across the four major web browsers. The source code of my analysis is provided in **Appendix B**.

[180] Chrome version 125, Safari version 16.1, Edge version 125, Firefox version 126.

[181] My analysis focuses on the rows where [redacted]

[182] https://gs.statcounter.com/browser-market-share/all/united-states-of-america.

83. The following table reports whether the seven data categories are collected by TikTok on riteaid.com, one of the six websites. It is evident that there is no substantial variability in TikTok Pixel's collection of the seven data categories from riteaid.com across the four web browsers. The results are similar for the other six websites – i.e., there is no substantial variability in TikTok Pixel's collection of the seven default data categories across the four web browsers.

	Chrome	Safari	Edge	Firefox
Timestamp	✓	✓	✓	✓
IP Address	✓	✓	✓	✓
User Agent	✓	✓	✓	✓
Cookies[183]	✓	✓	✓	✓
URL[184]	✓	✓	✓	✓
Event Information[185]	✓	✓	✓	✓
Content Information[186]	✓	✓	✓	✓

[183] Third-party cookie, First-party cookie, or Session ID.

[184] Page URL or Referrer URL.

[185] Event or Message ID.

[186] content_data or properties.

84. The following table reports the percentage of URLs where each of the seven data categories are collected by TikTok. It is evident that there is [redacted] in TikTok Pixel's collection of the seven data categories across the four web browsers.

	Chrome	Safari	Edge	Firefox
Timestamp[187]	[redacted]	[redacted]	[redacted]	[redacted]
IP Address[188]	[redacted]	[redacted]	[redacted]	[redacted]
User Agent[189]	[redacted]	[redacted]	[redacted]	[redacted]
Cookies[190]	[redacted]	[redacted]	[redacted]	[redacted]
URL[191]	[redacted]	[redacted]	[redacted]	[redacted]
Event Information[192]	[redacted]	[redacted]	[redacted]	[redacted]
Content Information[193]	-	-	-	-

85. It is again important to recognize that the percentages reported here are on a per-webpage basis, not on a per-user basis. This distinction is important because the probability that there exists a website visitor for whom TikTok has not collected all categories of data is practically zero. Concretely, from the following table, the probability that TikTok Pixel does not collect URL on one webpage is [redacted], on any of two or more webpages is 0.0%.[194] Given that TikTok Pixel collects data on hundreds of thousands of websites and a non-TikTok user (or class member) would

[187] In the column [redacted] of TIKTOK-BG-0124043.

[188] In the column [redacted] of TIKTOK-BG-0124043.

[189] In the column [redacted] of TIKTOK-BG-0124043.

[190] [redacted] column of TIKTOK-BG-0124043.

[191] [redacted] column of TIKTOK-BG-0124043.

[redacted] column of TIKTOK-BG-0124043.

[193] The data produced by TikTok (TIKTOK-BG-0124043) from the [redacted]) of the webpage content in one of the four standard formats (e.g., JSON-LD, OpenGraph), that TikTok Pixel automatically collects in POST request transmissions to https://analytics.tiktok.com/api/v2/pixel/act.

[194] Ross, S.M., 2014. Introduction to probability models. Academic press.

have visited many websites over the Class Period,[195,196] I can conclude that TikTok Pixel has collected URL from 100% of class members.

86. After reviewing the testimony of Defendants' corporate representative Branky Shao, which [redacted] with TikTok's previous representation that the [redacted] field in TIKTOK-BG-0124043 identifies that TikTok was [redacted],[197] I repeated the same analysis described above using another set of conditions to filter unmatched data.[198] The results are nearly identical and my conclusions do not change.

---

[195] https://trends.builtwith.com/websitelist/TikTok-Conversion-Tracking-Pixel/United-States.

[196] https://www.nerdydata.com/reports/tiktok-pixel/de68a0d2-1056-47f0-aec4-6f705982fc81.

[197] Feb. 27, 2024 Email from Defendants' Counsel K. Yin to Plaintiffs' Counsel G. Park.

[198] Criteria to identify unmatched data: [redacted]

- TIKTOK-BG-000160822 at -825 (script for Nov. 30, 2023 processed data); Tr. of 30(b)(6) Branky Shao Depo. (June 7, 2024) ("Shao Tr.") at 158:21-25 ([redacted] ").
- TIKTOK-BG-000160822 at -825; Shao Tr. at 158:21-25 ("[redacted]
- TIKTOK-BG-000160822 at -825; Shao Tr. at 159:23-25 [redacted] ").
- TIKTOK-BG-000160822 at -825; Shao Tr. at 158:13-20 ("[redacted]
- TIKTOK-BG-000003214 at -215.
- Shao Tr. at 189:17-20 [redacted]); *see also id.* [redacted] *Accord* Feb. 27, 2024 Email from Defendants' Counsel K. Yin to Plaintiffs' Counsel G. Park [redacted]

VI. UNIFORMITY IN TIKTOK PIXEL'S DATA STORAGE

87. TikTok stores non-TikTok user data collected through the Pixel and Events API for at least [redacted]. As TikTok stated in its response to Interrogatory No. 6: [redacted] [199] TikTok continued: [redacted]

- TIKTOK-BG-000160822 at -825 (script for Nov 30, 2023 processed data); Shao Tr. at 160:14-19 [redacted]; *see also id.*
- TIKTOK-BG-000160822 at -825 (script for Nov 30, 2023 processed data); Shao Tr. at [redacted]; *see also id.*
- Shao Tr. at [redacted]").

[199] Amended Response to Interrogatory No. 6 (Apr. 16, 2024).

[redacted]."[200]

88. It is important to note, however, that when TikTok says data is "[redacted]" after some period of time, it does not mean that the data is [redacted]. Rather, "[redacted]"[201] As an employee commented on this policy, "[redacted]" does not mean that the [redacted] Defendants' corporate representative testified that, in this "[redacted]" form, TikTok stores non-TikTok user data for [redacted].[203]

89. TikTok may have stored non-TikTok user data, [redacted]. One internal document suggests that the [redacted].[204]

VII. UNIFORMITY IN TIKTOK'S USAGE OF NON-TIKTOK USER DATA COLLECTED THROUGH THE PIXEL AND EVENTS API

90. The publicly stated purpose of TikTok's data collection is for advertising. TikTok explains that the TikTok Pixel is used to "Measure traffic on your website," "Measure ad campaign

[200] *Id.* (emphasis added).

[201] TIKTOK-BG-000002930 at -938.

[202] *Id.*

[203] Shao Tr. at 94:3-8 (testifying that [redacted]).

[204] TIKTOK-BG-000002930 at -930.

performance," and "Optimize your campaigns and find new customers."[205] TikTok further describes that TikTok Pixel "collects customer data and browsing behavior from your store to optimize your ad targeting experience," that it "tracks your ads' impact on your website," and that it "can help measure campaign performance and better define your ad's audience."[206]

91. Internally, TikTok discusses [redacted] including being able to process the data [redacted][207]

92. Consistent with its documents, TikTok has stated in interrogatory responses in this litigation that non-TikTok user data [redacted] in the following ways:

- [redacted];
- [redacted]
- [redacted];
- [redacted].[208]

93. I understand from counsel that discovery generally, and discovery into the uses of non-TikTok user data in particular, is ongoing. I reserve the right to amend, modify, and

[205] https://ads.tiktok.com/help/article/tiktok-pixel.

[206] https://ads.tiktok.com/help/article/data-sharing-tiktok-pixel-partners.

[207] TIKTOK-BG-000002930 at -932.

[208] Amended Response to Interrogatory No. 8 (Apr. 16, 2024).

supplement the opinions on TikTok's usage of class member data should new information become available to me.

VIII. CLASS MEMBER IDENTIFICATION OR VERIFICATION

94. I have been asked by counsel to investigate whether it is possible to identify or verify Class Members, i.e., non-TikTok users in the United States whose data is collected by TikTok Pixel during the Class Period, which I understand from counsel is March 2022 to the present.

95. First, given the sheer scale of TikTok Pixel's data collection on hundreds of thousands of websites, [209,210] it is unlikely that there are a non-trivial number of Internet users in the United States for whom TikTok Pixel has not collected data at least once during the Class Period.

a. Specifically, Dambra et al. found that even niche trackers that are present on 1-5% of the websites covered approximately at least 95% of the 250 thousand users once or more over the duration of just eight days.[211]

b. Extrapolating from this study, it is reasonable to conclude that there exist only a trivial number of Internet users in the United States for whom TikTok Pixel has not collected data over the span of the whole Class Period, which spans many more weeks and months than just eight days in the aforementioned research study.

c. Therefore, a simple way to objectively identify or verify class and subclass members is to check whether their email address exists in the list of email addresses

[209] https://trends.builtwith.com/websitelist/TikTok-Conversion-Tracking-Pixel/United-States.

[210] https://www.nerdydata.com/reports/tiktok-pixel/de68a0d2-1056-47f0-aec4-6f705982fc81.

[211] Dambra, S., Sanchez-Rola, I., Bilge, L. and Balzarotti, D., 2022. When Sally met trackers: Web tracking from the users' perspective. In 31st USENIX Security Symposium (USENIX Security).

of TikTok account holders in the United States. If the email address does not exist in the list, then that person is a class or subclass member.

96. Second, given that TikTok stores the data it collects from non-TikTok users for at least some period of time (see, for example, TIKTOK-BG-0124043), there is an even more precise way to identify or verify class members.[212] I describe that data and the class member identification/verification procedure below.

a. TikTok stores the processed data it collects from TikTok Pixel in the [redacted][213] that includes:

i. [redacted]

ii. [redacted]

iii. [redacted]; and

[212] I understand that TikTok has stated that it deletes data collected from non-TikTok users after 14 or 30 days and so the class member identification approach I describe here can be applied only to the data that TikTok has preserved. Of course, were TikTok preserving the non-TikTok user data, my proposed approach could be applied to a wider base of data to potentially identify more class members.

[213] In the Amended Response to Interrogatory no. 6, TikTok explains: [redacted]

[214] As discussed earlier, TikTok Pixel also collects [redacted]

[215] TikTok explained that "[redacted]" describes the [redacted] It further explained: [redacted]

2024 Email from Defendants' Counsel K. Yin to Plaintiffs' Counsel G. Park.

[216] TIKTOK-BG-0124043.

iv. [redacted].[217]

b. This data can be used to identify or verify class members as follows:

i. A person submits their email address,[218] phone number,[219] or TikTok cookies from their web browser's cookie jar.[220]

ii. If the email address, phone number, or TikTok cookies exist in the TikTok data for the rows that are labeled as unmatched,[221,222] then the person is a class member.

c. Using this procedure, my analysis shows that [redacted]

[217] If "[redacted]" then the data was collected by TikTok Pixel. If "[redacted]" then the data was collected by TikTok Events API.

[218] TikTok stores the [redacted] in the "[redacted]" table (TIKTOK-BG-0124043). Therefore, one would first compute [redacted] in the [redacted]" column.

[219] TikTok stores the [redacted] in the "[redacted]" table (TIKTOK-BG-0124043). Therefore, one would first compute [redacted] in the [redacted]" column.

[220] TikTok cookies are stored in the web browser's cookie jar for at least 13 months. *See* https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en.

[221] My analysis of TIKTOK-BG-0124043 showed that [redacted] of the US ([redacted] TikTok Pixel data [redacted] produced by TikTok has [redacted]

[222] My analysis of TIKTOK-BG-0124043 showed that [redacted] of the US [redacted] TikTok Pixel data [redacted] produced by TikTok has [redacted]

[redacted]

[redacted] 223,224

IX. COMPARABILITY OF DATA

83. I have been asked by counsel to assess the comparability of the data that TikTok collects through the Pixel and Events API and data collected by Google Ipsos Screenwise. While Google does not make publicly available the exact data fields it collects from panelists who participate in Screenwise, based on public disclosures available, I conclude that the data collected by Google appears comparable to the default categories of data collected by the TikTok Pixel.

---

223 My analysis of TIKTOK-BG-0124043 showed that the percentage of rows containing the following identifiers for the US [redacted] TikTok Pixel data [redacted] with [redacted] is:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

224 My analysis of TIKTOK-BG-0124043 showed that the percentage of rows containing the following identifiers for the US [redacted] TikTok Pixel data [redacted] with [redacted] is:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

84. I understand that Screenwise[225] is a panel that Google built to "learn more about how everyday people use the Internet."[226] Google sought volunteers to serve as panelists who would "add a browser extension that will share with Google the sites you visit and how you use them."[227] In exchange, the panelists received Amazon.com gift cards.[228] In a Google Panel Privacy Policy, Google described that the data collected from Screenwise panelists may include every web page visited and all interactions (e.g., mouse clicks) with those webpages, including URL and IP addresses and the length of time you spent visiting websites; data about the browser used by panelist and his or her browser settings; and cookies.[229]

85. These categories are substantially similar to the seven data categories collected by TikTok Pixel. As discussed above, these categories include URL, IP Address, Timestamp, User Agent (which identifies website visitor's operating system, vendor, browser, and browser version), and Cookies. *See supra* at Section V.A. Through the category that I labeled Content Information, TikTok Pixel also collects data on website visitors' interactions with webpages on which the Pixel is installed by auto-scraping metadata and inferring button clicks.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed this 21st day of June, 2024, in Davis, California.

Zubair

Zubair Shafiq, Ph.D.

[225] There exist other similar panels such as SavvyConnect (https://surveysavvy.com/savvyconnect), which are not specifically tied to Google, that similarly collect data from panelists.

[226] https://web.archive.org/web/20120210041154/http:/www.google.com/landing/screenwisepanel/.

[227] *Id.*

[228] *Id.*

[229] https://screenwisepanel.com/google-panel-privacy-policy.

APPENDIX A

Zubair Shafiq

3043 Kemper Hall
Davis, CA, 95616 USA
zubair@ucdavis.edu
www.cs.ucdavis.edu/~zubair

Research Interests

Web Privacy, Internet Measurement, Internet Security, Computer Networks

Professional Experience

2020– **Associate Professor**
Department of Computer Science, University of California-Davis

2014–2020 **Assistant Professor**
Department of Computer Science, University of Iowa

2009–2014 **Research Assistant**
Department of Computer Science and Engineering, Michigan State University

2013 **Research Intern**
IBM T. J. Watson Research Center

2012 **Research Intern**
Telefonica Research

2011 **Research Intern**
AT&T Labs – Research

2007-2009 **Research Engineer**
Next Generation Intelligent Networks Research Center, Pakistan

Education

2009–2014 **Ph.D. Computer Science**
Department of Computer Science and Engineering, Michigan State University

2004–2008 **B.E. Electrical Engineering**
National University of Sciences & Technology (NUST), Pakistan

Honors and Awards

2024 **Caspar Bowden Award**, Runner-up for Outstanding Research in Privacy Enhancing Technologies
2023 **Best Paper Award**, ACM Internet Measurement Conference
2023 **Chancellor's Fellow**, University of California Davis
2020 **Research Highlights**, Communications of the ACM
2020 **Dean's Scholar Award**, University of Iowa
2018 **NSF Faculty Early Career Development (CAREER) Award**
2018 **Andreas Pfitzmann Award**, Best Student Paper at Privacy Enhancing Technologies Symposium
2017 **Best Paper Award**, ACM Internet Measurement Conference
2015 **NSF CISE Research Initiation Initiative (CRII) Award**
2013 **Fitch-Beach Outstanding Graduate Research Award**, Michigan State University
2012 **Best Paper Award**, IEEE International Conference on Network Protocols

2007, 2008 **Dean's Plaque of Excellence**, National University of Sciences & Technology, Pakistan

Publications

CCS **Blocking Tracking JavaScript at the Function Granularity**
Abdul Haddi Amjad, Shaoor Munir, Zubair Shafiq, Muhammad Ali Gulzar
ACM Conference on Computer and Communications Security, 2024 (in press)

USENIX Security **PURL: Safe and Effective Sanitization of Link Decoration**
Shaoor Munir, Patrick Lee, Umar Iqbal, Zubair Shafiq, Sandra Siby
USENIX Security Symposium, 2024 (in press)

JETLaw **Google's Chrome Antitrust Paradox**
Shaoor Munir, Konrad Kollnig, Anastasia Shuba, Zubair Shafiq
Vanderbilt Journal of Entertainment and Technology Law, 2024 (in press)

IMWUT/ UbiComp **Aragorn: A Privacy-Enhancing System for Mobile Cameras**
Hari Venugopalan, Zainul Abi Din, Trevor Carpenter, Jason Lowe-Power, Sam King, Zubair Shafiq
ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2024 (in press)

CHI **Understanding Underground Incentivized Review Services**
Rajvardhan Oak, Zubair Shafiq
ACM Conference on Human Factors in Computing Systems, 2024

S&P **The Inventory is Dark and Full of Misinformation: Understanding the Abuse of Ad Inventory Pooling in the Ad-Tech Supply Chain**
Yash Vekaria, Rishab Nithyanand, Zubair Shafiq
IEEE Symposium on Security & Privacy, 2024

JOLT **A Scientific Approach to Tech Accountability**
Woodrow Hartzog, Scott Jordan, David Choffnes, Athina Markopoulou, Zubair Shafiq
Beyond the FTC: The Future of Privacy Enforcement, Harvard Journal of Law & Technology, 2023

PNAS **Auditing YouTube's Recommendation System for Ideologically Congenial, Extreme, and Problematic Recommendations**
Muhammad Haroon, Magdalena Wojcieszak, Anshuman Chhabra, Xin Liu, Prasant Mohapatra, Zubair Shafiq
Proceedings of the National Academy of Sciences (PNAS), 2023

IMC **Tracking, Profiling, and Ad Targeting in the Alexa Echo Smart Speaker Ecosystem**
Umar Iqbal, Pouneh Nikkhah Bahrami, Rahmadi Trimananda, Hao Cui, Alexander Gamero-Garrido, Daniel Dubois, David Choffnes, Athina Markopoulou, Franziska Roesner, Zubair Shafiq
ACM Internet Measurement Conference, 2023
Best Paper Award

PETS **A Utility-Preserving Obfuscation Approach for YouTube Recommendations**
Jiang Zhang, Hadi Askari, Konstantinos Psounis, Zubair Shafiq
Privacy Enhancing Technologies Symposium, 2023

PETS **Blocking JavaScript without Breaking the Web**
Abdul Haddi Amjad, Zubair Shafiq, Muhammad Ali Gulzar
Privacy Enhancing Technologies Symposium, 2023

CCS **CookieGraph: Measuring and Countering First-Party Tracking Cookies**
Shaoor Munir, Sandra Siby, Umar Iqbal, Steven Englehardt, Zubair Shafiq, Carmela Troncoso
ACM Conference on Computer and Communications Security, 2023

S&P **Accuracy-Privacy Trade-off in Deep Ensemble: A Membership Inference Perspective**
Shahbaz Rezaei, Zubair Shafiq, Xin Liu
IEEE Symposium on Security & Privacy, 2023

USENIX Security **AutoFR: Automated Filter Rule Generation for Adblocking**
Hieu Le, Salma Elmalaki, Athina Markopoulou, Zubair Shafiq
USENIX Security Symposium, 2023

NDSS **Harpo: Learning to Subvert Online Behavioral Advertising**
Jiang Zhang, Konstantinos Psounis, Muhammad Haroon, Zubair Shafiq
Network and Distributed System Security Symposium, 2022

USENIX Security **WebGraph: Capturing Advertising and Tracking Information Flows for Robust Blocking**
Sandra Siby, Umar Iqbal, Steven Englehardt, Zubair Shafiq, Carmela Troncoso
USENIX Security Symposium, 2022

USENIX Security **Khaleesi: Breaker of Advertising and Tracking Request Chains**
Umar Iqbal, Charlie Wolfe, Charles Nguyen, Steven Englehardt, Zubair Shafiq
USENIX Security Symposium, 2022

PETS **FP-Radar: Longitudinal Measurement and Early Detection of Browser Fingerprinting**
Pouneh Nikkhah Bahrami, Umar Iqbal, Zubair Shafiq
Privacy Enhancing Technologies Symposium, 2022

ACL **Adversarial Authorship Attribution for Deobfuscation**
Wanyue Zhai, Jonathan Rusert, Zubair Shafiq, Padmini Srinivasan
Association for Computational Linguistics, 2022

ACL **On the Robustness of Offensive Language Classifiers**
Jonathan Rusert, Zubair Shafiq, Padmini Srinivasan
Association for Computational Linguistics, 2022

EuroS&P **DNN Model Architecture Fingerprinting Attack on CPU-GPU Edge Devices**
Kartik Patwari, Syed Mahbub Hafiz, Han Wang, Houman Homayoun, Zubair Shafiq, Chen-Nee Chuah
IEEE European Symposium on Security and Privacy, 2022

DATE **Stealthy Inference Attack on DNN via Cache-based Side-channel Attacks**
Han Wang, Syed Mahbub Hafiz, Kartik Patwari, Chen-Nee Chuah, Zubair Shafiq, Houman Homayoun
IEEE/ACM Design Automation and Test in Europe, 2022

IMC **TrackerSift: Untangling Mixed Tracking and Functional Web Resources**
Abdul Haddi Amjad, Danial Saleem, Fareed Zaffar, Muhammad Ali Gulzar, Zubair Shafiq
ACM Internet Measurement Conference, 2021

S&P **Fingerprinting the Fingerprinters: Learning to Detect Browser Fingerprinting Behaviors**
Umar Iqbal, Steven Englehardt, Zubair Shafiq
IEEE Symposium on Security & Privacy, 2021

NDSS **CV-Inspector: Towards Automating Detection of Adblock Circumvention**
Hieu Le, Athina Markopoulou, Zubair Shafiq
Network and Distributed System Security Symposium, 2021

EACL **Through the Looking Glass: Learning to Attribute Synthetic Text Generated by Language Models**
Shaoor Munirl, Brishna Batool, Zubair Shafiq, Padmini Srinivasan, Fareed Zaffar
European Chapter of the Association for Computational Linguistics, 2021

IMC **Understanding Incentivized Mobile App Installs on Google Play Store**
Shehroze Farooqi, Alvaro Feal, Tobias Lauinger, Damon McCoy, Zubair Shafiq, Narseo Vallina-Rodriguez
ACM Internet Measurement Conference, 2020

ACL **A Girl Has A Name: Detecting Authorship Obfuscation**
Asad Mahmood, Zubair Shafiq, Padmini Srinivasan
Annual Conference of the Association for Computational Linguistics, 2020

S&P **AdGraph: A Graph-Based Approach to Ad and Tracker Blocking**
Umar Iqbal, Peter Snyder, Shitong Zhu, Benjamin Livshits, Zhiyun Qian, Zubair Shafiq
IEEE Symposium on Security & Privacy, San Francisco, 2020

PETS **CanaryTrap: Detecting Data Misuse by Third-Party Apps on Online Social Networks**
Shehroze Farooqi, Maaz Musa, Zubair Shafiq, Fareed Zaffar
Privacy Enhancing Technologies Symposium, Montreal, 2020

PETS **Inferring Tracker-Advertiser Relationships in the Online Advertising Ecosystem**
John Cook, Rishab Nithyanand, Zubair Shafiq
Privacy Enhancing Technologies Symposium, Montreal, 2020

PETS **The TV is Smart and Full of Trackers: Measuring Smart TV Advertising and Tracking**
Janus Varmarken, Hieu Le, Anastasia Shuba, Zubair Shafiq, Athina Markopoulou
Privacy Enhancing Technologies Symposium, Montreal, 2020

IoTDI **Characterizing Smart Home IoT Traffic in the Wild**
M. Hammad Mazhar, Zubair Shafiq
ACM/IEEE Conference on Internet of Things Design and Implementation, Sydney, 2020

PAM **FlowTrace: A Framework for Active Bandwidth Measurements using In-band Packet Trains**
Adnan Ahmed, Ricky Mok, Zubair Shafiq
Passive and Active Measurement Conference, Eugene, 2020

PETS **A Girl Has No Name: Automated Authorship Obfuscation using X-Mutant**
Asad Mahmood, Faizan Ahmad, Zubair Shafiq, Padmini Srinivasan, Fareed Zaffar
Privacy Enhancing Technologies Symposium, Stockholm, 2019

PETS **No Place to Hide: Inadvertent Location Privacy Leaks on Twitter**
Jonathan Rusert, Osama Khalid, Dat Hong, Zubair Shafiq, Padmini Srinivasan
Privacy Enhancing Technologies Symposium, Stockholm, 2019

WWW **Measurement and Early Detection of Third-Party Application Abuse on Twitter**
Shehroze Farooqi, Zubair Shafiq
The Web Conference (WWW), San Francisco, 2019

WWW **ShadowBlock: A Lightweight and Stealthy Adblocking Browser**
Shitong Zhu, Umar Iqbal, Zhongjie Wang, Zhiyun Qian, Zubair Shafiq, Weiteng Chen
The Web Conference (WWW), San Francisco, 2019

WWW **Measuring Political Personalization of Google News Search**
Huyen Le, Raven Maragh, Brian Ekdale, Timothy Havens, Andrew High, Zubair Shafiq
The Web Conference (WWW), San Francisco, 2019

ASONAM **A Postmortem of Suspended Twitter Accounts in the 2016 U.S. Presidential Election**
Huyen Le, Bob Boynton, Zubair Shafiq, Padmini Srinivasan
IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), Vancouver, 2019

TDSC **Large Scale Characterization of Software Vulnerability Life Cycles**
Muhammad Shahzad, Zubair Shafiq, Alex X. Liu
IEEE Transactions on Dependable and Secure Computing, 2019

PETS **NoMoAds: Effective and Efficient Cross-App Mobile Ad-Blocking**
Anastasia Shuba, Athina Markopoulou, Zubair Shafiq
Privacy Enhancing Technologies Symposium, Barcelona, 2018
Andreas Pfitzmann Best Student Paper Award

NDSS **Measuring and Disrupting Anti-Adblockers Using Differential Execution Analysis**
Shitong Zhu, Xunchao Hu, Zhiyun Qian, Zubair Shafiq, Heng Yin
Network and Distributed System Security Symposium, San Diego, 2018

INFOCOM **Real-time Video Quality of Experience Monitoring for HTTPS and QUIC**
M. Hammad Mazhar, Zubair Shafiq
IEEE International Conference on Computer Communications, Honolulu, 2018

TON **Optimizing Internet Transit Routing for Content Delivery Networks**
Faraz Ahmed, Zubair Shafiq, Amir Khakpour, Alex Liu
IEEE/ACM Transactions on Networking, 2018

TBD **Optimizing Taxi Driver Profit Efficiency: A Spatial Network-based Markov Decision Process Approach**
Xun Zhou, Huigui Rong, Chang Yang, Qun Zhang, Amin Vahedian Khezerlou, Hui Zheng, Zubair Shafiq, Alex Liu
IEEE Transactions on Big Data, 2018

TOPS **Measuring, Characterizing, and Detecting Facebook Like Farms**
Muhammad Ikram, Lucky Onwuzurike, Shehroze Farooqi, Emiliano De Cristofaro, Arik Friedman, Guillaume Jourjon, Dali Kaafar, Zubair Shafiq
ACM Transactions on Privacy and Security, 2017

TIST **A Traffic Flow Approach to Early Detection of Gathering Events: Comprehensive Results**
Amin Khezerlou, Xun Zhou, Lufan Li, Zubair Shafiq, Alex X. Liu, Fan Zhang
ACM Transactions on Intelligent Systems and Technology, 2017

IMC **Measuring and Mitigating OAuth Access Token Abuse by Collusion Networks**
Shehroze Farooqi, Fareed Zaffar, Nektarios Leontiadis, Zubair Shafiq
ACM Internet Measurement Conference, London, 2017
Best Paper Award
CACM Research Highlights 2020

IMC **The Ad Wars: Retrospective Measurement and Analysis of Anti-Adblock Filter Lists**
Umar Iqbal, Zubair Shafiq, Zhiyun Qian
ACM Internet Measurement Conference, London, 2017

SIGMETRICS **Characterizing and Modeling Patching Practices of Industrial Control Systems**
Brandon Wang, Xiaoye Li, Leandro P. de Aguiar, Daniel S. Menasche, Zubair Shafiq
ACM International Conference on Measurement and Modeling of Computer Systems, Urbana-Champaign, 2017

PETS **Detecting Anti Ad-blockers in the Wild**
Muhammad Haris Mughees, Zhiyun Qian, Zubair Shafiq
Privacy Enhancing Technologies Symposium, Minneapolis, 2017

ICDM **Accurate Detection of Automatically Spun Content via Stylometric Analysis**
Usman Shahid, Shehroze Farooqi, Raza Ahmad, Zubair Shafiq, Padmini Srinivasan, Fareed Zaffar
IEEE International Conference on Data Mining, New Orleans, 2017

CHI **Revisiting The American Voter on Twitter**
Huyen Le, G.R. Boynton, Yelena Mejova, Zubair Shafiq, Padmini Srinivasan
ACM Conference on Human Factors in Computing Systems, Denver, 2017

ICDCS **Distributed Load Balancing in Key-Value Networked Caches**
Sikder Huq, Zubair Shafiq, Sukumar Ghosh, Amir Khakpour, Harkeerat Bedi
IEEE International Conference on Distributed Computing Systems, Atlanta, 2017

ICNP **Peering vs. Transit: Performance Comparison of Peering and Transit Interconnections**
Adnan Ahmed, Zubair Shafiq, Harkeerat Bedi, Amir Khakpour
IEEE International Conference on Network Protocols, Toronto, 2017

ICNP **Suffering from Buffering? Detecting QoE Impairments in Live Video Streams**
Adnan Ahmed, Zubair Shafiq, Harkeerat Bedi, Amir Khakpour
IEEE International Conference on Network Protocols, Toronto, 2017

ICNP **Multipath TCP Traffic Diversion Attacks and Countermeasures**
Ali Munir, Zhiyun Qian, Zubair Shafiq, Alex Liu, Franck Le
IEEE International Conference on Network Protocols, Toronto, 2017

ICWSM **Scalable News Slant Measurement Using Twitter**
Huyen Le, Zubair Shafiq, Padmini Srinivasan
AAAI International Conference on Web and Social Media, Denver, 2017

HT **Bumps and Bruises: Mining Presidential Campaign Announcements on Twitter**
Huyen Le, G.R. Boynton, Yelena Mejova, Zubair Shafiq, Padmini Srinivasan
ACM Conference on Hypertext and Social Media, Prague, 2017

Networking **Cascade Size Prediction in Online Social Networks**
Zubair Shafiq, Alex Liu
IFIP Networking, Prague, 2017
Best Paper Award Candidate (3 nominations out of 43 accepted papers)

Networking **A Graph Theoretic Approach to Fast and Accurate Malware Detection**
Zubair Shafiq, Alex Liu
IFIP Networking, Prague, 2017

eCrime **Characterizing Key Stakeholders in an Online Black-Hat Marketplace**
Shehroze Farooqi, Muhammad Ikram, Emiliano De Cristofaro, Arik Friedman, Guillaume Jourjon, Dali Kaafar, Zubair Shafiq, Fareed Zaffar
IEEE/APWG Symposium on Electronic Crime Research, Prague, 2017

ICNP **Optimizing Internet Transit Routing for Content Delivery Networks**
Faraz Ahmed, Zubair Shafiq, Amir Khakpour, Alex Liu
IEEE International Conference on Network Protocols, Singapore, 2016

DSN **Malware Slums: Measurement and Analysis of Malware on Traffic Exchanges**
Salman Yousaf, Umar Iqbal, Shehroze Farooqi, Raza Ahmad, Zubair Shafiq, Fareed Zaffar
IEEE/IFIP International Conference on Dependable Systems and Networks, France, 2016

SIGMETRICS **QoE Analysis of a Large-Scale Live Video Streaming Event**
Adnan Ahmed, Zubair Shafiq, Amir R. Khakpour
ACM International Conference on Measurement and Modeling of Computer Systems, France, 2016

ICDCS **The Internet is For Porn: Measurement and Analysis of Online Adult Traffic**
Faraz Ahmed, Zubair Shafiq, Alex X. Liu
IEEE International Conference on Distributed Computing Systems, Japan, 2016

INFOCOM **Characterizing Caching Workload of a Large Commercial Content Delivery Network**
Zubair Shafiq, Amir R. Khakpour, Alex X. Liu
IEEE International Conference on Computer Communications, San Francisco, 2016

SIGSPATIAL **A Traffic Flow Approach to Early Detection of Gathering Events**
Xun Zhou, Amin Vahedian Khezerlou, Alex Liu, Zubair Shafiq, Fan Zhang
ACM International Conference on Advances in Geographic Information Systems, San Francisco, 2016

CIKM **The Rich and the Poor: A Markov Decision Process Approach to Optimizing Taxi Driver Revenue Efficiency**
Huigui Rong, Xun Zhou, Chang Yang, Zubair Shafiq, Alex Liu
ACM International Conference on Information and Knowledge Management, Indianapolis, 2016

TON **Characterizing and Optimizing Cellular Network Performance during Crowded Events**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Shobha Venkataraman, Jia Wang
IEEE/ACM Transactions on Networking, 2016

SMP **What Campaigns Become as Social Media Become the Infrastructure of Political Communication**
G.R. Boynton, Huyen Le, Yelena Mejova, Zubair Shafiq, Padmini Srinivasan
Social Media and Politics, 2016

TMC **Geospatial and Temporal Dynamics of Application Usage in Cellular Data Networks**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang
IEEE Transactions on Mobile Computing, 2015

NSF/FCC QoE **Tracking Mobile Video QoE in the Encrypted Internet**
Zubair Shafiq
NSF/FCC Workshop on Tracking Quality of Experience in the Internet, Princeton, 2015

NSF/FCC QoE **Bidirectional Crosslayer QoE Optimization**
Srikanth Sundaresan, Zubair Shafiq
NSF/FCC Workshop on Tracking Quality of Experience in the Internet, Princeton, 2015

IMC **Paying for Likes? Understanding Facebook Like Fraud Using Honeypots**
Emiliano De Cristofaro, Arik Friedmam, Guillaume Jourjon, Dali Kaafar, Zubair Shafiq
ACM Internet Measurement Conference, 2014

SIGMETRICS **Understanding the Impact of Network Dynamics on Mobile Video User Engagement**
Zubair Shafiq, Jeffrey Erman, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang
ACM International Conference on Measurement and Modeling of Computer Systems, 2014

SIGMETRICS **Revisiting Caching in Content Delivery Networks**
Zubair Shafiq, Alex X. Liu, Amir Khakpour
ACM International Conference on Measurement and Modeling of Computer Systems, 2014

SIGMETRICS **A First Look at Cellular Network Performance during Crowded Events**
Zubair Shafiq, Alex X. Liu, Amir Khakpour
ACM International Conference on Measurement and Modeling of Computer Systems, 2013

ICNP **Who are You Talking to? Breaching Privacy in Encrypted IM Networks**
Muhammad U. Ilyas, Zubair Shafiq, Alex X. Liu, Hayder Radha
IEEE International Conference on Network Protocols, 2013

CSCW **Is News Sharing on Twitter Ideologically Biased?**
Jonathan Morgan, Cliff Lampe, Zubair Shafiq
ACM Conference on Computer Supported Cooperative Work and Social Computing, 2013

ACM HotNets **Cross-Path Inference Attacks on Multipath TCP**
Zubair Shafiq, Franck Le, Mudhakar Srivatsa, Alex X. Liu
ACM Workshop on Hot Topics in Networks, 2013

TON **Large Scale Measurement and Characterization of Cellular Machine-to-Machine Traffic**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang
IEEE/ACM Transactions on Networking, 2013

JSAC **Identifying Leaders and Followers in Online Social Networks**
Zubair Shafiq, Muhammad U. Ilyas, Alex X. Liu, Hayder Radha
IEEE Journal on Selected Areas in Communications, 2013

JSAC **A Distributed Algorithm for Identifying Information Hubs in Social Networks**
Muhammad U. Ilyas, Zubair Shafiq, Alex X. Liu, Hayder Radha
IEEE Journal on Selected Areas in Communications, 2013

JNSM **TCAMChecker: A Software Approach to the Error Detection and Correction of TCAM-based Networking Systems**
Zubair Shafiq, Chad Meiners, Alex Liu, Ke Shen, Zheng Qin
Springer Journal of Network and Systems Management, 2012

ICNP **A Semantics Aware Approach to Automated Reverse Engineering Unknown Protocols**
Yipeng Wang, Xiaochun Yun, Zubair Shafiq, Alex X. Liu, Zhibin Zhang, Liyan Wang, Danfeng (Daphne) Yao, Yongzheng Zhang, Li Guo
IEEE International Conference on Network Protocols, 2012
Best Paper Award

SIGMETRICS **A First Look at Cellular Machine-to-Machine Traffic – Large Scale Measurement and Characterization**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang
ACM International Conference on Measurement and Modeling of Computer Systems, London, 2012

ICSE **A Large Scale Exploratory Analysis of Software Vulnerability Life Cycles**
Muhammad Shahzad, Zubair Shafiq, Alex X. Liu
International Conference on Software Engineering, Switzerland, 2012

INFOCOM **Characterizing Geospatial Dynamics of Application Usage in a 3G Cellular Data Network**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang
IEEE Conference on Computer Communications, Orlando, 2012

SIGMETRICS **Characterizing and Modeling Internet Traffic Dynamics of Cellular Devices**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jia Wang
ACM International Conference on Measurement and Modeling of Computer Systems, San Jose, 2011

Networking **A Random Walk Approach to Modeling the Dynamics of the Blogosphere**
Zubair Shafiq, Alex X. Liu
IFIP Networking, Spain, 2011

INFOCOM **A Distributed and Privacy-Preserving Algorithm for Identifying Information Hubs in Social Networks**
Muhammad U. Ilyas, Zubair Shafiq, Alex X. Liu, Hayder Radha
IEEE Conference on Computer Communications, Spain, 2011

RAID **PE-Miner: Mining Structural Information to Detect Malicious Executables in Realtime**
Zubair Shafiq, Syeda Momina Tabish, Fauzan Mirza, Muddassar Farooq
International Symposium On Recent Advances In Intrusion Detection, France, 2009

GECCO **Evolvable Malware**
Sadia Noreen, Shafaq Murtaza, Zubair Shafiq, Muddassar Farooq
ACM Genetic and Evolutionary Computation Conference, Canada, 2009

CCS AISec **Using Spatio-Temporal Information in API Calls with Machine Learning Algorithms for Malware Detection and Analysis**
Faraz Ahmed, Haider Hameed, Zubair Shafiq, Muddassar Farooq
Workshop on Security and Artificial Intelligence, ACM Conference on Computer & Communications Security, Chicago, 2009

KDD CSI **Malware Detection using Statistical Analysis of Byte-Level File Content**
Syeda Momina Tabish, Zubair Shafiq, Muddassar Farooq
Workshop on CyberSecurity and Intelligence Informatics (CSI), ACM Conference on Knowledge Discovery and Data Mining, France, 2009

VB **PE-Probe: leveraging packer detection and structural information to detect malicious portable executables**
Zubair Shafiq, Syeda Momina Tabish, Muddassar Farooq
Virus Bulletin, Switzerland, 2009

Elsevier **Fuzzy Case Based Reasoning for Facial Expression Recognition**
Aasia Khanum, Muid Mufti, M. Y. Javed, Zubair Shafiq
Elsevier Fuzzy Sets and Systems, 2009

EvoComNet **A Comparative Study of Fuzzy Inference Systems, Neural Networks and Adaptive Neuro Fuzzy Inference Systems for Portscan Detection**
Zubair Shafiq, Muddassar Farooq, Syed Ali Khayam
Applications of Evolutionary Computing, EvoComNet, Italy, 2008

DIMVA **Embedded Malware Detection using Markov n-grams**
Zubair Shafiq, Syed Ali Khayam, Muddassar Farooq
International Conference on Detection of Intrusions, Malware and Vulnerability Assessment, France, 2008

GECCO **Improving Accuracy of Immune Inspired Malware Detectors using Intelligent Features**
Zubair Shafiq, Syed Ali Khayam, Muddassar Farooq
ACM Genetic and Evolutionary Computation Conference, Atlanta, 2008

Funding

External Competitive Research Grants

UC **Auditing Compliance of Data Privacy Laws in California**
UC Partnerships in Computational Transformation
PI, Duration: 2022-2023, Total: $160,000, Share: $80,000
Personnel: Zubair Shafiq (PI: UC Davis); Athina Markopoulou (PI: UC Irvine); Gene Tsudik (Co-PI: UC Irvine)

NSF-SaTC **Defending against Emerging Stateless Web Tracking**
National Science Foundation
PI, Duration: 2022-2026, Total: $1,200,000, Share: $400,000
Personnel: Zubair Shafiq (PI: UC Davis); Alexandros Kapravelos (PI: NC State); Anupam Das (Co-PI: NC State)

CITRIS and the Banatao Institute **Auditing the compliance of California consumer privacy regulations at scale**
Center for Information Technology Research in the Interest of Society (CITRIS)
Co-PI, Duration: 2021-2022, Total: $60,000, Share: $20,000
Personnel: Serge Egelman (Co-PI: UC Berkeley); Zubair Shafiq (Co-PI: UC Davis)

NSF-SaTC-Frontier **Protecting Personal Data Flow on the Internet**
National Science Foundation
PI, Duration: 2020-2025, Total: $10,000,000, Share: $1,100,000
Personnel: Zubair Shafiq (PI: UC Davis); Athina Markopoulou (PI: UC Irvine); Konstantinos Psounis (PI: USC); David Choffnes (PI: Northeastern)

NSF-CAREER **Quality of Experience and Network Management in the Encrypted Internet**
National Science Foundation
PI, Duration: 2018-2023, Total: $500,000, Share: $500,000
Personnel: Zubair Shafiq (PI: UC Davis)

NSF-SaTC **A Multi-Layer Learning Approach to Mobile Traffic Filtering**
National Science Foundation
PI, Duration: 2018-2021, Total: $500,000, Share: $250,000
Personnel: Zubair Shafiq (PI: UC Davis); Athina Markopoulou (PI: UC Irvine)

NSF-SaTC **The Web Ad Technology Arms Race: Measurement, Analysis, and Countermeasures**
National Science Foundation
PI, Duration: 2017-2020, Total: $500,000 + $16,000 (REU Supplement 2019) + $16,000 (REU Supplement 2021), Share: $282,000
Personnel: Zubair Shafiq (PI: UC Davis); Zhiyun Qian (PI: UC Riverside)

NSF-NeTS **Towards Scalable and Energy Efficient Cellular IoT Communication**
National Science Foundation
PI, Duration: 2016-2019, Total: $500,000, Share: $166,000
Personnel: Zubair Shafiq (PI: Iowa); K.K. Ramakrishnan (PI: UC Riverside); Koushik Kar (PI: RPI)

NSF-SaTC **Multipath TCP Side Channel Vulnerabilities and Defenses**
National Science Foundation
PI, Duration: 2015-2018, Total: $500,000, Share: $167,000
Personnel: Zubair Shafiq (PI: Iowa); Zhiyun Qian (PI: UC Riverside); Alex Liu (PI: Michigan State University)

NSF-NeTS **Towards Measurement and Optimization of Internet Video Quality of Experience**
National Science Foundation
PI, Duration: 2015-2018, Total: $175,000 + $16,000 (REU Supplement 2016), Share: $191,000
Personnel: Zubair Shafiq (PI: Iowa)

DTL **Detection and Circumvention of Ad-Block Detectors**
Data Transparency Lab
PI, Duration: 2016-2017, Total: $56,000, Share: $28,000
Personnel: Zubair Shafiq (PI: Iowa); Zhiyun Qian (PI: UC Riverside)

Internal Competitive Research Grants

Academic Senate **Socio-Computational Interventions to Mitigate Misinformation in Recommendations**
Noyce Foundation
PI, Duration: 2022-2023, Total: $25,000
Personnel: Magdalena Wojcieszak (PI), Zubair Shafiq (Co-PI)

Noyce **Measuring and Mitigating Biases in Social Recommendation Algorithms**
Noyce Foundation
PI, Duration: 2022-2023, Total: $236,000
Personnel: Zubair Shafiq (PI), Magdalena Wojcieszak (Co-PI)

Noyce **Cross-Layer Approach to Enhance Security/Privacy of AI-enabled IoT Eco-Systems**
Noyce Foundation
Co-PI, Duration: 2022-2023, Total: $225,000
Personnel: Chen-Nee Chuah (PI), Zubair Shafiq (Co-PI), Houman Homayoun (Co-PI)

Noyce **Measuring and Mitigating Biases in Social Recommendation Algorithms**
Noyce Foundation
PI, Duration: 2021-2022, Total: $235,690
Personnel: Zubair Shafiq (PI), Xin Liu (Co-PI), Magdalena Wojcieszak (Co-PI)

Noyce **Cross-Layer Approach to Enhance Security/Privacy of AI-enabled IoT Eco-Systems**
Noyce Foundation
Co-PI, Duration: 2021-2022, Total: $225,000
Personnel: Chen-Nee Chuah (PI), Zubair Shafiq (Co-PI), Houman Homayoun (Co-PI)

UIRF **Social Media Powered Real-Time Digital News Recommendation**
University of Iowa Research Foundation
PI, Duration: 2015-2016, Total: $75,000
Personnel: Zubair Shafiq (PI)

Obermann **Heterogeneous Network Data Analytics to Improve Urban Sustainability**
Obermann Center Interdisciplinary Research Grant
PI, Duration: 2015-2016, Total: $12,000
Personnel: Xun Zhou (PI); Zubair Shafiq (Co-PI)

Industry Grants and Unrestricted Gifts

Siemens PI, Duration: 2021, Total: $60,000, Share: $60,000
Personnel: Zubair Shafiq (PI: UC Davis)

Siemens PI, Duration: 2019, Total: $30,000, Share: $30,000
Personnel: Zubair Shafiq (PI: Iowa)

Siemens PI, Duration: 2018, Total: $60,000, Share: $60,000
Personnel: Zubair Shafiq (PI: Iowa)

Verizon PI, Duration: 2018, Total: $20,000, Share: $20,000
Personnel: Zubair Shafiq (PI: Iowa)

Minim PI, Duration: 2018, Total: $66,164, Share: $66,164
Personnel: Zubair Shafiq (PI: Iowa)

Siemens PI, Duration: 2017, Total: $30,000, Share: $30,000
Personnel: Zubair Shafiq (PI: Iowa)

Nokia PI, Duration: 2017, Total: $53,200, Share: $53,200
Personnel: Zubair Shafiq (PI: Iowa)

Futurewei PI, Duration: 2017, Total: $100,384, Share: $100,384
Personnel: Zubair Shafiq (PI: Iowa)

Facebook PI, Duration: 2016, Total: $8,400, Share: $8,400
Personnel: Zubair Shafiq (PI: Iowa)

Teaching

ECS 289M **Topics in Privacy**
Spring 2024, University of California at Davis

ECS 188 **Ethics in an Age of Technology**
Winter 2024, University of California at Davis

ECS 152A **Computer Networks**
Fall 2023, University of California at Davis

FYS **Big Data, Big Brother**
Winter 2023, University of California at Davis

ECS 289M **Network Security & Privacy**
Winter 2023, University of California at Davis

ECS 152A **Computer Networks**
Fall 2022, University of California at Davis

ECS 152A **Computer Networks**
Spring 2022, University of California at Davis

ECS 153 **Computer Security**
Winter 2022, University of California at Davis

ECS 289M **Data-Driven Security**
Spring 2021, University of California at Davis

ECS 152B **Computer Networks**
Winter 2021, University of California at Davis

CS 2620 **Networking & Security for Informatics**
Spring 2020, The University of Iowa

CS 4980 **Online Advertising & Tracking**
Fall 2019, The University of Iowa

CS 2620 **Networking & Security for Informatics**
Spring 2019, The University of Iowa

CS 4980 **Internet Measurement**
Fall 2018, The University of Iowa

CS 2620 **Networking & Security for Informatics**
Spring 2018, The University of Iowa

CS 2620 **Networking & Security for Informatics**
Spring 2017, The University of Iowa

CS 4980 **Network Security and Privacy**
Fall 2016, The University of Iowa

CS 2620 **Networking & Security for Informatics**
Spring 2016, The University of Iowa

CS 4980 **Advanced Computer Networks**
Fall 2015, The University of Iowa

CS 2620 **Networking & Security for Informatics**
Spring 2015, The University of Iowa

CS 4980 **Internet Measurement**
Fall 2014, The University of Iowa

Students

Doctorate

2022-current Rajvardhan Oak
2021-current Pouneh Nikkhah Bahrami
2021-current Shaoor Munir
2021-current Yash Vekaria
2016-2021 Dr. Umar Iqbal; First Position: CIFellow/Postdoc, University of Washington
2015-2021 Dr. Shehroze Farooqi; First Position: Researcher, Palo Alto Networks
2015-2019 Dr. Huyen Le; First Position: Postdoc, National Center for Toxicological Research

Select Recent Masters Mentees

2021 Mohammad Ismail Daud
2021 Sunshine Chong
2021 Rachit Dhamija
2020 Pouneh Nikkhah Bahrami

Select Recent Undergraduate Mentees

2023 Divya Raj
2023 Shuaib Ahmed
2023 Ryan Swift
2023 Tangbaihe Wang
2023 Patrick Lee
2022 Jake Smith
2022 Christina Phan
2022 Kev Rockwell
2020-2022 Kajal Patel (NSF REU)
2020-2022 Wanyue Zhai (graduate student at Stanford)
2020-2022 Ray Ngan (NSF REU) (industry: Palo Alto Networks)
2020-2021 Surya Konkimalla
2020-2021 Charles Nguyen (industry: Apple)
2019-2021 Charlie Wolfe (NSF REU) (industry: Apple)
2021 Caelan MacArthur (NSF DREU)
2020-2021 Taimur Kashif (NSF REU) (industry: VMWare)
2019-2020 Ashton Woiwood (NSF REU)
2017 Treyton Krupp (NSF REU)
2015 Mirza Besic

High School

2023 Reeva Rao

2023	Jayalakshmi Raffill
2019	Kathy Zhong
2018	Alice Martynova
2017	William Kim
2016	Brandon Wang

External Service

Conference TPC/Reviewer	IEEE S&P (2022), PETS (2021, 2020, 2019, 2018, 2017), ACM IMC (2021, 2020), ACM CoNEXT (2019), ACM SIGMETRICS (2023, 2022, 2020, 2013), WWW (2020, 2018), ACM CSCW (2018, 2019), IEEE/IFIP TMA (2020, 2019), NDSS MADWeb Workshop (2019), IEEE INFOCOM (2017, 2015, 2010, 2009), ACM WPES (2018), IEEE S&P Consumer Protection Workshop (2021, 2020), ACM SIGCOMM Internet-QoE Workshop (2017), ACM SIGCOMM Workshop on IoT Security and Privacy (2018), WWW CyberSafety Workshop (2018), WWW Workshop on Location and the Web (2018), IEEE ICNP (2014, 2013), MASCOTS (2013), ICDCN (2017, 2018)
Journal Reviewer	IEEE/ACM Transactions on Networking, ACM Transactions on the Web, IEEE Transactions on Mobile Computing, IEEE Transactions on Network and Service Management, ACM Transactions on Multimedia Computing, IEEE Transactions on Cognitive Communications and Networking, ACM SIGCOMM Computer Communication Review, Elsevier Computer Communications, Elsevier Performance Evaluation, Springer Wireless Networks
PC Co-Chair	Privacy Enhancing Technologies Symposium (PETs), 2025
PC Co-Chair	Privacy Enhancing Technologies Symposium (PETs), 2024
PC Co-Chair	Workshop on Technology and Consumer Protection (ConPro'23), IEEE Symposium on Security & Privacy ("Oakland")
PC Co-Chair	Workshop on Technology and Consumer Protection (ConPro'22), IEEE Symposium on Security & Privacy ("Oakland")
PC Co-Chair	Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb'23), Network and Distributed System Security Symposium (NDSS)
PC Co-Chair	Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb'22), Network and Distributed System Security Symposium (NDSS)
Publicity Co-Chair	ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT 2020)
Co-Chair	NSF NeTS Early Career Investigators Workshop 2019
PC Co-Chair	Student Workshop - ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT 2018)
PC Co-Chair	WWW 8th International Workshop on Location and the Web (LocWeb 2018)
Poster Chair	ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS 2018)
Technical Committee	Elsevier Computer Communications (2015-2019)
Guest Editor	Special Issue on Mobile Traffic Analytics, Elsevier Computer Communications (2016)
Editorial Board	Proceedings on Privacy Enhancing Technologies (PoPETs) (2019, 2020, 2021)

Panelist NSF (2017, 2018, 2019, 2020, 2021, 2022, 2023)

Internal Service

Chair Departmental Colloquium Series
Department of Computer Science, University of California Davis, 2021-

Member Diversity, Equity, Inclusion Committee
College of Engineering, University of California Davis, 2021-2022

Committee Departmental Graduate Committee
Department of Computer Science, University of Iowa, 2019-2020

Chair Departmental Colloquium Series
Department of Computer Science, University of Iowa, 2019-2020

Member Executive Committee, Iowa Initiative for Artificial Intelligence (IIAI)
The University of Iowa, 2019-2020

Member Department Executive Committee
Department of Computer Science, The University of Iowa, 2016-2019

Member Faculty Recruitment Committee
Department of Computer Science, The University of Iowa, 2015-2020

Mentor Black Girls Do Science
College of Engineering, The University of Iowa, 2015-2016

Mentor Iowa Edge Classroom Experience
Center for Diversity and Enrichment, The University of Iowa, 2015-2018

Mentor Summer Research Opportunities Program (SROP)
Graduate College, The University of Iowa, 2017

Mentor Secondary Student Training Program (SSTP)
Belin-Blank Center, The University of Iowa, 2016-2019

Patents

USPTO 10484881 Jia Wang, Lusheng Ji, Alex X. Liu, Zubair Shafiq. Optimization of cellular network architecture based on device type-specific traffic dynamics. November 2019

USPTO 10420167 Jia Wang, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Zubair Shafiq. Cellular Connection Sharing. September 2019

Expert Testimony & Reports (in the past five years)

4:20-cv-05146 **Calhoun et al. v. Google**

4:21-cv-02155 **In re Google RTB Consumer Privacy Litigation**

5:23-cv-02431 **In John Doe I et al. v. Google**

22-01-88230-D **State of Texas v. Google**

A 2002633 **Doe, et al. v. Bon Secours Mercy Health**

24-C-20-000591	**Doe, et al. v. Medstar Health**
19-2-26674-1	**Doe, et al. v. Virginia Mason**
23CV037304	**Doe, et al. v. Family Planning Associates Medical Group**
22-cv-03580	**In re Meta Pixel Healthcare Litigation**
23OT01-0026	**Stake et al. v. Knox**
23-cv-00964	**Bernadine Griffith v. TikTok**

Litigation Consulting (in the past five years)

Bleichmar Fonti & Auld

Simmons Hanly Conroy

Lieff Cabraser Heimann & Bernstein

DiCello Levitt Gutzler

Norton Rose Fulbright

Pritzker Levine

Social Media Victims Law Center

Girard Sharp

Hammond Law

Caddell & Chapman

Whatley Kallas

Office of the Attorney General, Texas

AZA Law

Susman Godfrey

APPENDIX B
(slipsheet)

Appendix B consists of source code, scripts, and data and has been produced, by email, in native form to Defendants.